Technology Espionage Analytical approach for Global Cyber Theft Strategy in Red China Rising Commercial Organization

Dr. Hafiz Gulfam Ahmad Umar

Department of Computer Science and IT.
Faculty of Science, The Ghazi University, D.G. khan.

Abstract
The quantification of economic impact of cyber security is a challenging task in a globalized world. According to the cyber security surveys, the emerging countries are more vulnerable to cyber threats in spite of widespread awareness. China is determined and active in developing its own IT industry. It is also isolating itself from international IT technology and uses of IT in their economic regions like business. China developed its business sector with the jaunt hands of IT as applying cyber security. Application of cyber security in business sector of china has its own value. SWOT analysis was applied for verdict of cyber security in chines business sector. Cyber security Stenting's values show 80 percent business become more secure but on the other hand 20 percent threating situations have to face. Bulks of opportunities are still in vacant situation in case of cyber security presentations in chines business.

Keywords:
Cyber security, China business organizations. Swot analysis

1. Introduction

Technology is an important part for every small or big business organization. Definitely use of internet has brought about numerous benefits to businesses but it has also opened up new vulnerabilities and points of violence. The development and deployment of new technologies has been accompanied every step of the IT industry (David Emm, Kaspersky Lab). Internet provide connectivity to a large number of infrastructures via corporate networks. Cyber security is, therefore, a vital entity of the different sector of emerging economies. A strong interest in cybersecurity has initiated research aimed at assessing the maturity of national cyber security(Bilge Karabacakn, SevgiOzkanYildirim). It is assumed that cyber attacks occur everywhere on a mass scale daily around the world, and companies with limited information information usually show when they become victims of cybercrime and the fact that some attacks are difficult to track.

Figure 1 shows a description of 20 countries around the world in cybercrime in the world. In a computational context, cyber security is a technological approaches and ,methods planned to defend networks, data and software, personal computers, from destruction or illegal access. Different cyber systems represents the underlying infrastructures to cyber threats that are asymmetric in nature. A cyber-attack has the obvious advantages of privacy, affordability, deniability and ease of use matched with conventional attacks (A.Chan,E.Yung,P.Lam,C).

Indeed Cyber-criminals increasingly target business organizations because these are perceived to have the weakest defenses. Numerous Chinese telecommunication companies such as Huawei have been disqualified from contracting and attaining any broadband network providers in the US and Australia (Stark, Jill). It appears that the Chinese offensive cyber capabilities develop, unwilling the West to accept any growing danger to its private information, cyber infrastructure or security in general (David E., and Nicole, (2016).There is compelling evidence that at present business organizations are not implementing all the required security measures to protect themselves, despite significant efforts by official bodies and security professionals to improve resilience(Karen 2016). The incidence of cybercrime has merged with people's perception of real-world risks.

The related online vulnerabilities and people's perceptions of those dangers are even concealing real-life threats for some. Within the last year 689 million peoples 21 countries experience cyber crime. Since 2015 cybercrime victims spend $126 BILLION globally (Norton Cyber Security Insights Report 2016).

Manuscript received November 5, 2025
Manuscript revised November 20, 2025
https://doi.org/10.22937/IJCSNS.2025.25.11.15

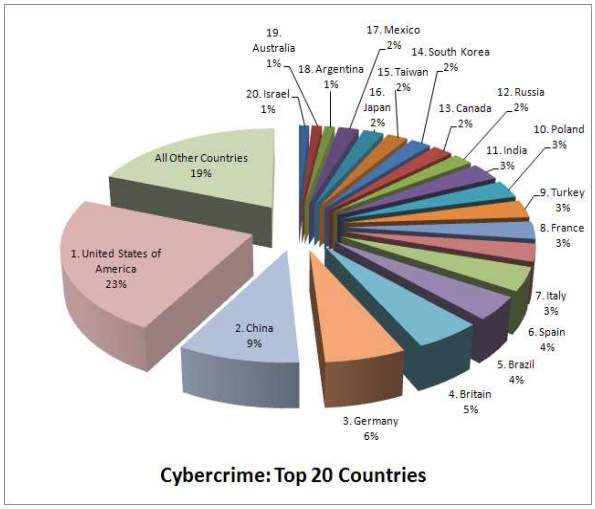

Figure 1 Cyber Crime rate Top 20 Countries by Symantec Report 2016

In emerging countries especially rapid progressive economy of China, business organizations have already spent a huge amount averting data theft and other cyber space attacks. In spite of Chinese local (technology and telecom companies') efforts to supply high quality products for domestic and commercial use, a large component of technology connected to Chinese networks still instigates from the West. Chinese official's authorities are influenced that these systems are fortified with Trojan horses and loopholes to steal China's national secrets and avoid its further economic upsurge (Ernst, Dieter). The estimated budgets of Information security of Chinese companies was about $8 million in the year 2016, which is considerably higher than the global average of $ 5.1 million, (Gao Yuan). Cyber attacks are becoming a daily reality for all business organizations and individuals, but, as a rule, do not understand the numerous categories of bouts, features and potential consequences that can become an hurdle to the defense of information security (M. Uma and G. Padmavathi). The study began with a close review of the current position of cybercriminals, especially in China, based on a appraisal of particular global prose, together with an scrutiny of the key proceedings of current years. The objective was to acquire a overall impression of cyber security, understand the ways of working and the potential impact on businesses or individuals, and countermeasures that needed to be taken to eliminate risks. Studies aimed at cyber security and attacks have been identified and traced in recent years in China. Data was calculated on the basis of the report of Symantec for 2016 and China Cyber Security report 2016. When assessing the various internal and external factors that may affect cyber security in a business enterprise, one of the best basic assessment models used is the SWOT analysis. In this study, we will provide a complete overview of how to create a SWOT analysis using some very simple methods. It was incredible for writers to achieve a comprehensive set of data for investigation purposes. In this article, we apply SWOT analysis to know the strength, weakness, opportunities and threats to cyber security. Nevertheless, the study is based on information obtained as a result of aggregating data on the breaches perceived and tracked over the past two years, collected from the history of updates and attacks, from reviews and reports released by global major market participants. There are four dimensional objective of this study that are given below

- Strengthen value of Cyber Security in business of China
- Weakness of Cyber Security in business of China
- Opportunities of Cyber Security in business of China
- Threat of Cyber Security in business of China

2. RESEARCH METHODOLOGY

The study commenced with cyber security in business sector. Business sector is the important segment of economy that controls a big portion of economical progressive approach. In this modern phase of financial prudence every economy desires to update with new technologies but everything has its own porn and crones that have an effective share in their values. As the evaluation of specialized international literature, include legal aspects and study cyber security is going to introduce with rapid involvement in this global village. For the analysis of this cyber security approach in business sector a social measuring practice with the name of SWOT analysis is going to apply here. The basic purpose of this analysis slant is to find brief review of concerning research area in four dimensions. These dimensions are given below with their forthcoming determinations. Strengths, Weakness, Opportunist, Threats.

.

2.11 LEGISLATION TO MAKE STRENGTHEN CHINESE CYBER SECURITY

All over the world as commercial organization has moved towards the global digital world, lawbreakers have developed refined criminal ecosystem that functions much like any business management structure. To compete with this risk, cybersecurity has become a hot topic. Like other countries in the world, China is also fully aware of the

importance of cybersecurity and has a prominent place in national security. China also launched its leading group to strengthen cybersecurity for the emerging business environment. In February 2024, a well-known organization on cybersecurity and informatization was set up, headed by President Xi Jinping. In addition, cyber security was involved in the current administration performance report submitted by Prime Minister Li Keqiang. In 2015, the NPC Standing Committee in early July revised the law on cybersecurity and feedback to researchers. It is assumed that security laws will be announced earlier with the sanction of the law on cybersecurity. In June 2016, the Standing Committee of the NPC held a subsequent analysis of the Cyber security Law and explained the need to protect key information, infrastructure and confidential data. In July 2016, the additional version of the Cybersecurity Rule was legitimately issued on the NPC web and provided.

By established a law on cybersecurity, the government sought to highlight the monitoring bodies responsible for controlling cybersecurity in China. The following agencies are mentioned as regulatory bodies. These governing bodies make stronger cybersecurity in China:

3. WEAKNESSES OF CYBER SECURITY IN CHINESE BUSINESS SECTOR.

Commercial organizations in China in a number of industries, including e-commerce, insurance, information technology, banking, tourism and automotive, education, control more and more personal information and transaction data. Cyber-attacks subject to these business organizations and sensitive data is often leaked by vulnerabilities in the organizational system. These weaknesses include:

1. Unsatisfactory control over the security of data transmission, security management and access control to confidential data during conversion, storage or use can be missed intentionally.
2. The second drawback is the lack of capabilities of security services and incident response, that creates problems for organizations so that they can effectively respond to potential security threats.
3. The third flaw found in Chinese resources is dedicated to fixing data leakage channels after the the general public (NPC). The proposed law on cybersecurity provides for the localization of data, research and requirements for valid names. The Cybersecurity Act. Bill,

- Safeguard China's cyber sovereignty;
- Protection beside cyber-attacks;
- Enhance Internet security and safety;
- Regulate the use of personal data.

The Cyber Security Act 2016 is an important milestone in the development of cybersecurity in China. In the second draft of the Cybersecurity Law, organizations of all industries should focus on the following points.

are detected, which lead to further attacks, leading to leakage of even more sensitive data.

4. To ensure that it is difficult for organizations to respond to cyber attack that manage weak organizational security operations and security architectures.

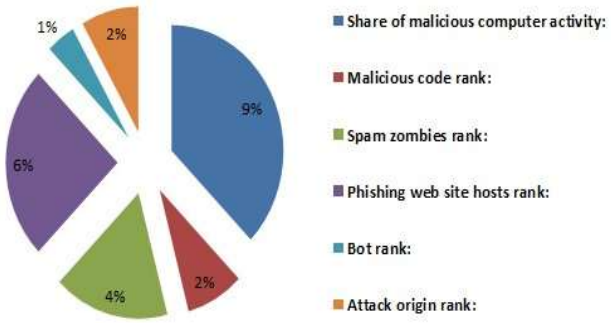

Figure 2 Contributing factors in China

Fig. 2. Includes six factors: the percentage of malicious activity on the computer, the rating of malicious code, the rating of zombie spam, the phishing rating of the website, the rank of the bot and the source of the attack, to justify the rating of cybercrime. During our discussions with industry representatives, they believe that they can include the main factors in the corporate sector, which lead to a weaker underreporting. Heads of IT departments may not dare to notify top management, for fear of criticism. Some business organizations do not care about the importance of cybersecurity, and they do not know about violations and other incursions, some notaries can recommend to their

clients that they are not in the best legal interest to inform senior management about such cybercrimes.

Figure 3 Major factors enhance Cyber victimization.

Under-reporting may also be convoyed by the under-investigation of cybercrime by corporate victims. According to statistical parameters, Internet users in China mourn financial losses to 91.5 billion yuan due to the leakage of personal information, fraud, junk mail, etc. (KPMG Cyber security in China). Over the last twelve months,

4. OPPORTUNITIES OF CYBER SECURITY IN CHINESE BUSINESS ORGANIZATION

A little bit difficult to understanding China's cyber structure, strategies and organization. The Chinese have not traditional and comprehensive approach to cyber issues in the form of a strategy. The number of internet users has already exceeded 3.4 billion due to a big populated country, 721 million internet populations coming from China (Internet Live state 2016). Naturally, China is increasingly reliant on on various cyber assets and the Chinese establishments have reacted accordingly. We have observed a growing importance on cyber security measures, as well as an increase in the country's enthusiasm to take advantage of the opportunities that the internet provides, and to respond to the terrorizations it poses to national security. With the leading population in the world, China holds a generous pool of experts with potential value for the government and its cyber operations in business sector. From business perspective *Cyber Security Provide opportunities to* regulators in various industries, Some details contians:

- Audit of information technology
- Continuity of business
- Migration and maintenance of systems development,
- Outsourcing of management,
- Information security
- Information technology management,

The banking sector business is the most sustainable industry. The CBRC carries out both field and off-site evaluations and regular audits based on cybersecurity requirements. The results of the assessment will affect the level of compliance of each bank. The focus of external principles in the banking industry has shifted from "managing IT risks" to more specific topics, including business continuity, outsourcing risk management and technological manageability. IT, healthcare and manufacturing enterprises , manage the security of their applications and IT infrastructure based on measures to ensure the protection of information security,

5. CYBER THREATS MAKE ESSENTIAL CYBER SECURITY.

Cybercrime is increasing every year, every day, even a second, by 2017, it is expected that the global market for cybersecurity will grow to 120.1 billion dollars. In 2011, it was $ 63.7. The projected annual cost of global cybercrime is $ 100 billion. Read our info graphics to find out the latest statistics and trends in the cybercrime industry. The cyber infrastructure is designated as a acute structure if its destruction or damage will have detrimental consequences for the economy, social order or national security of the country or any business organization (ABI Research 2014).

Ever day More than 600,000 Facebook accounts are compromised, Intruders hacked 15% of users of social networks reported that their profiles were hacked... 1 out of 10 social network users said they were a victim of fraud or fake links on social networking platforms (Go Gulf). According to different reports the figures founds for the past 12 months 2016 was very horrible.

In the China, a huge amount financial losses of up to 91.5 billion Yuan suffered by internet users. due to leakage of personal information, Internet fraud, junk e-mail, etc. During the first half of 2016, 84% were faced with some negative impact of personal information breach and 37% of Internet users grieved from economic losses due to various types of Internet vulnerabilities (Cyber security in China).Hackers deceive the IP address for hindering any criminal acivity, This kind of attack called spoofing. In spoofing attacker detection (Özçelik and Brooks, 2015). Non-targeted attacks still account for the majority of malicious attacks, which increased by 26 percent in 2014. In fact, last year, more than 317 million new malicious programs were created. Every day about one million new threats were issued. Some of these attacks can not be a direct risk to organizations. In addition to the irritating factor for IT, this affects the productivity of employees and diverts IT resources that could be better spent on high-level security problems (ISTR 2015). The list of cyber attacks is described in Table 4, which can affect the organization of the business.

Table 1 Summary of threating factors in cyber security

1	Reconnaissance attacks	Kinds of attack by illegal detection and comparison with numerous type of data.
2	Access attacks	Device access gained by intruder
3	Denial of service	Intrusion in the system make it to be too busy or full to handle requests Invasion of the system full for processing requests to makes it too busy
4	Active attacks	All parties Attack with data transmission
5	Attacks in MANET	Attack with aims to slow or stop the flow of information
6	Attacks on WSN	Sensors used preventing , detecting and transmitting attack
7	Man in the middle attack	Two communication ends used attacker interferes when every message sent from source A to source B
8	Cyber crime	To stop users for gain materialistic with computers
9	Cyber espionage	Use of internet to spy
10	Passive attacks	Attack with eaves dropping without meddling with the database
11	Cyber terrorism	cyber space use for creating large scale destruction.
12	Cyber war	Disruption Act of a nation with the

6. CONCLUSION

As a concluding remark on Cyber security regarding China's business sector there is no National security without cyber security. China is determinedly moving forward to develop its own IT industry. By exercising legislation to control over major state-run businesses stream lining their cyber space and developing parallel standards in the software and hardware sectors. In addition, to further enhance China's independence in IT sector, alternate standards for encryption, new operating systems and competing app stores are developed. However, insufficient quality regulations are posing a hazard to IT security. Chinese internet users are vulnerable by a shadow IT economy. Pirated programs without having security updates are often installed on computers. These insecure computers are more prone to hackers and can be used as a base for worldwide attacks. Protection of individual privacy has attracted global attention, It assumed that the individual privacy protection in China will become tougher with the increase in the cost of meeting the requirements for

enterprises, which as a result of this increase. In orde
follow China, as in other areas, Pakistan can also incre
the IT sector there and save cyberspace by enacting law
cybersecurity.

REFERENCE

[1] Karen Renaud," How smaller businesses struggle with security advice" Computer Fraud & Security,Volume 2016, Issue 8, August 2016, Pages 10–18

[2] David Emm, Kaspersky Lab,(2013) Security for SMBs: why it's not just big businesses that should be concerned. Computer Fraud & Security, Volume 2013, Issue 4, April 2013, Pages 5-8

[3] *PwC, CIO, and CSO (2012) Global State of Information Security Survey*.

[4] http://www.pwc.com/us/en/view/issue-15/cybersecurity-business-priority.html

[5] Klaus Julisch,(2013) Understanding and overcoming cyber security anti-patterns Computer Networks, Volume 57, Issue 10, Pages 2206-221

[6] www.compuvaultstl.com/wp-content/.../SMB_Guide_to_Cyber_Security_2016.pdf

[7] Uma, M., Padmavathi, G.,(2013). A survey on various cyber-attacks and their classification, International Journal of Network Security, 15.

[8] Mihail Antonescua , Ramona Birău ,(2015) Financial and non-financial implications of cybercrimes in emerging countries. Procedia Economics and Finance 32 (2015) 618 – 621

[9] Raiyn, J., (2014). A survey of cyber attack detection strategies. Int. J. Security Appl. 8 (1), 247–256.

[10] ABI Research, Global Cybersecurity Index: Conceptual Fra- mework, London, United Kingdom, 2014.

[11] Hafiz Gulfam Ahmad,(2013) Current Cloud Computing Security Concerns from Consumer Perspective Hydromechatronics Engineering, Vol. 41, No. 24. ISSN. 1001-3881, 2013.24.001 December 2013.

[12] Özçelik, I., Brooks, R.R., 2015. Deceiving entropy based DoS detection. Computer Security 48, 234–245.

[13] Gaurav Somani, Manoj Singh Gaur,(2016) DDoS attacks **in cloud computing: Collateral damage to non-targets** ,Computer Networks, Volume 109, Part 2, 9 November 2016, Pages 157-17.

[14] Symentic internet-security-threat-report-volume-20-2015.

[15] http://www.brighthub.com/computing/smb-security/articles/2259.aspx

[16] Humphrey, Albert (December 2005). "SWOT Analysis for Management Consulting"(PDF). SRI Alumni Newsletter. SRI International.

[17] **Jump up** "Albert Humphrey The "Father" of TAM". TAM UK. Retrieved 2012-06-03.

[18] Gao Yuan(2015) Cybersecurity market growing in China. China Daily.

[19] Bilge Karabacakn, SevgiOzkanYildirim, A vulnerability-driven cyber security maturity model for measuring national critical infrastructure protection preparedness. International journal of critical infrastructure protection 15 .

[20] A.Chan,E.Yung,P .Lam, C.TamandS. Cheung,Application of Delphi methods in selection of Procurement systems for construction projects, Construction Management and Economics, vol. 19(7),pp.699–718,2001.

[21] KPMG Cyber security in China 2016.

[22] https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2016/08/cyber-security-in-china.pdf

[23] Li Keqiang,Report on the Work of the Government(2016) Fourth Session of the 12th National People's Congress of the People's Republic of China on March 5, 2016

[24] Norton Cyber Security Insights Report 2016.

[25] http://www.go-gulf.com/blog/cyber-crime/

[26] Grauman, Brigid. Cyber-security: The Vexed Question of Global Rules. Report by Security & Defence Agenda, 2012, p. 55. 8

[27] David Bandurski, cited in Lococo, Edmond, and Keith Zhai. 'China Seeks Global Internet Influence at CEO Forum on Canal Bank.' Bloomberg Technology. 18 Nov. 2014. Accessed 18 Aug. 2016.

[28] Internet Live Stats compiles data from six major reliable agencies, including the International Telecommunications Unit and the World Bank. See more at 'China Internet Users.' Internet Live Stats, 2016. Accessed 18 Aug. 2016.

[29] Stark, Jill. 'US Follows Australia in Naming Huawei as a Possible Security Threat.' The Sydney Morning Herald. 9 Oct. 2012. Accessed 18 Aug. 2016.

[30] http://www.smh.com.au/it-pro/security-it/us-follows-australia-in-naming-huawei-as-a-possible-security-threat-20121007-277ad.html.

[31] 6 David E., and Nicole, (2016) The US National Security Agency (NSA) has itself hacked into computers belonging to Huawei and China Telecom, a fact that became public with the Snowden leaked documents evidencing the American worldwide online spying. See more at Sanger, Perlroth. 'N.S.A. Breached Chinese Servers Seen as Security Threat.' The New York Times. 22 Mar. 2014. Accessed 18 Aug. 2016.

[32] http://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html?_r=0.