Human Factor of Online Social Media Cybersecurity Risk Impact on Critical National Information Infrastructure

Nik Zulkarnaen Khidzir, Ahmad Rasdan Ismail, Khairul Azhar Mat Daud, Mohamad Shahfik Affendi Abdul Ghani, Suriatini Ismail and Asrul Hery Ibrahim

Abstract Social Digital Media become an effective platform for many cyber community to promote product and services to get reach greater potential market around the globe. However, Social Digital Media could lead to several critical cybersecurity risk that might be difficult to manage and mitigate. Moreover, some the cybersecurity risk could cause severe impact of human factors especially if the risk affected the Critical National Information Infrastructure (CNII) that serve as backbone of the country. Hence the objective of the research are to determine the human factors related of social media cybersecurity risk and; to discuss their severity level impact on Critical National Information Infrastructure (CNII). Questionnaires are distributed to various private and government agencies practitioners for the study. The finding of the research show that the top 5 most critical cybersecurity risk are Information Theft; Cyber Attacks; Cyber Crime; Information Manipulation; Productivity Loss. This article also highlight top 5 least critical

N.Z. Khidzir (✉) · A.R. Ismail · K.A.M. Daud · M.S.A.A. Ghani · S. Ismail
Global Entrepreneurship Research and Innovation Centre,
Universiti Malaysia Kelantan, Bachok, Kelantan, Malaysia
e-mail: zulkarnaen.k@umk.edu.my

A.R. Ismail
e-mail: rasdan@umk.edu.my

K.A.M. Daud
e-mail: azhar.md@umk.edu.my

M.S.A.A. Ghani
e-mail: afendi.ag@umk.edu.my

S. Ismail
e-mail: suriatini@umk.edu.my

N.Z. Khidzir
Faculty of Creative Technology and Heritage, Universiti Malaysia Kelantan,
Bachok, Kelantan, Malaysia

A.H. Ibrahim
Faculty of Business and Entrepreneurship, Universiti Malaysia Kelantan,
Kota Bharu, Kelantan, Malaysia
e-mail: hery.i@umk.edu.my

D. Nicholson (ed.), *Advances in Human Factors in Cybersecurity*,
Advances in Intelligent Systems and Computing 501,
DOI 10.1007/978-3-319-41932-9_16

cybersecurity risks which are Attack of the Software; Cyber Assault/Bullying; Espionage; Terrorisms; Risk of Losing the legal Battle. Through the findings, expert, management and practitioner would be able to identify critical cybersecurity risk and address them appropriately and effectively.

Keywords Cybersecurity risk · Human factor · Social media · Critical national information infrastructure · Severity impact level

1 Introduction

Nowadays, the benefit of participating in social media not only involve simple social interaction, but also building reputations and bridging in career opportunities, and/or generating direct monetary revenue [1] It's considered to be the greatest technological invention ever discovered, social digital media are fast gaining popularity globally among online cyber community. Social Media can also serve as tools facilitating intra- and inter-organization activities among peers, customers, business partners, and organizations [2]. Unfortunately, Social Digital Media could lead to several critical cybersecurity risks that could cause serious impact of the Critical National Information Infrastructure (CNII) sector. National Defense and Security; Banking and Finance; Information and Communications; Energy; Transportation; Water; Health Services; Government; Emergency Services; Food and Agriculture that might be difficult to manage and mitigate were the focus area of Critical National Information Infrastructure.

The current advanced Information Communication Technology (ICT) allowed several cybersecurity risks occur and effected the entire activities within Critical National Information Infrastructure sectors. If this occur it's could be a serious disaster for the entire information infrastructure ecosystem. Moreover, some the cybersecurity risk could cause severe impact of human factors that are vital to their incapacity or destruction would have a devastating impact on National economic strength; National image; National Defense and Security; Government capability to function; Public health and safety. Therefore, this study aims to measure the level of Information Security Risk severity level on Critical National Information Infrastructure (CNII) in the context of Malaysian. The findings could be serve as a fundamental study, and to stimulate innovative ideas in the future research in this body of knowledge.

The paper is organized as follows: the next section briefly describes the literature review on Social Media, Cybersecurity Risk Factors, and Critical National Information Infrastructure (CNII). The third section highlight several related issues on social media and cybersecurity risks in critical national information infrastructure. The forth section describes the methodology and research model used in the study. The fifth section further discusses the results and findings from the study. The final section is devoted to the conclusion and a discussion of contribution and future direction of the study.

2 Related Literature Review

Online Social Digital Media become an effective platform for many businesses, especially cyberpreneur to promote their product and services to capture greater potential market across the globe. Besides the advantages, functions and capability offered by this technology, it's comes with several issues and challenge that need to overcome in the appropriate manner so that the real benefit of Online Social Media will be fully utilized by cyber community. Fundamental concept and related previous literature for this study had been identified as the basis for this study. This section analyzed and discussed several related literature and concept used for this study.

2.1 Online Social Media Networking

Online Social Media as "a group of Internet-based applications that build on the ideological and technological foundations of Web 2.0, and allow the creation and exchange of user generated content" [3]. Social Media define as the set of Web-based broadcast technologies that enable the democratization of content, giving people the ability to emerge from consumers of content to publishers [4]. Through the Social Media platform, users creates online communities to share information, ideas, personal messages, and other content [5].

The dramatic development of social media has helped shape people's connections with others via different social media platforms [6]. Social media drive a new set of models for various kinds of businesses that challenge traditional business processes and operations [7]. Individuals and/or organizations therefore must be well prepared to embrace the challenges and opportunities brought about by social media [2]. Generally, social media considered as part of the internet society ecosystem that serve an effective communication channel for cyber community. Besides the unbelievable opportunities offered through this technology, cybersecurity risks considered as emergent challenges to look into seriously.

2.2 Information Security and Cybersecurity Risk Factors

Besides the excitement sharing information about their activities, status, location, feeling, etc., they are not realizing that the information that they share in Online Media Social could contribute to the cybersecurity risks that might be difficult to manage and mitigate. The similar principles of information security risk [8] was adopted to redefine the new term of cybersecurity risks nature. Cybersecurity risks are the chances of electronic forms of threats action on core principles of information security [9] such confidentiality, integrity, availability to cause impact contributed to security incidents. In a computing context, the term security implies cybersecurity from both aspect of technology and human factors. These both aspect of cybersecurity could also consider among challenging issues among Online Social Media users to manage and mitigate.

Based on the literature, 18 common cybersecurity risk factors had been identified for the purpose of this study. There are Identity Theft [10–13]; Information manipulation [10, 14, 15]; Cyber Assault/Bullying [10, 15]; Advanced Persistence Threats [10, 15]; Information Theft [10, 15]; Cyber Crime [10, 11, 16]; Insider [10, 16]; Espionage [10, 13]; Cyber Attacks [10, 15]; Transactional [10, 16, 17]; Attack of the Software [10, 11, 17]; Terrorisms [10, 13, 17]; Phishing Pond [10, 15]; Privacy Violation [10, 15]; Risk of Losing the Legal Battle [10, 13]; Corporate Espionage [10, 13]; Viruses and Malware [10, 11]; Productivity Loss [10].

2.3 Critical National Information Infrastructure (CNII)

The term "information infrastructure" has been increasingly used to refer to integrated solutions based on the now ongoing fusion of information and communication technologies [18]. The term became popular after the US plan for National Information Infrastructures (NII) was launched. The term has been widely used to describe national and global communication networks like the Internet and more specialized solutions for communications within specific business sectors [18]. The growing researchers interest for information infrastructure has produced a rich variety of studies and analyses of information infrastructures.

In India, National Cyber Security Policy 2013 [19] was introduce to protect the public and private infrastructure from cyber attacks [20]. The policy also intends to safeguard "information, such as personal information (of web users), financial and banking information and sovereign data". Knowing the Cyberspace is a complex environment consisting of interactions between people, software services supported by worldwide distribution of information and communication technology [20–22]. The main purpose of the policy development is to protect their country Critical National Information Infrastructure.

In Malaysia, Cyber Security Malaysia adopted the similar concept of information infrastructure to describe Critical National Information Infrastructure (CNII) definition. Critical National Information Infrastructure (CNII) is defined as those assets (real and virtual), systems and functions that are vital to the nations that their incapacity or destruction would have a devastating impact on the following aspects:

- National economic strength [23]; Confidence that the nation's key growth area can successfully compete in global market while maintaining favourable standards of living.
- National image [23]; Projection of national image towards enhancing stature and sphere of influence.

- National defence and security [23]; guarantee sovereignty and independence whilst maintaining internal security.
- Government capability to functions [23]; maintain order to perform and deliver minimum essential public services.
- Public health and safety [23]; delivering and managing optimal health care to the citizen.

At this moment, Cyber Security Malaysia had classified 10 Critical National Information Infrastructure focuses Sectors. There are National Defense and Security; Banking and Finance; Information and Communications; Energy; Transportation; Water; Health Services; Government; Emergency Services; Food and Agriculture [23].

Since these 10 sectors considered as the Critical National Information Infrastructure, its could explore several significant results and valuable findings. Therefore, this study will analyzed the Severity level of cybersecurity risk factors on Critical National Information Infrastructure. Details result of the analysis will be discuss further through this article.

3 Social Media Cybersecurity Risk Issues on Critical National Information Infrastructure

Cybersecurity is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access [11, 24]. Social Digital Media could lead to several critical cybersecurity risks that could cause serious impact of the Critical National Information Infrastructure (CNII) sector, such National Defense and Security; Banking and Finance; Information and Communications; Energy; Transportation; Water; Health Services; Government; Emergency Services; Food and Agriculture [23] that might be difficult to manage and mitigate. Moreover, some the cybersecurity risk could cause severe impact of human factors that are vital to their incapacity or destruction would have a devastating impact on National economic strength; National image; National Defense and Security; Government capability to function; Public health and safety [23].

National Defense and Security considered as one of the Critical National Information Infrastructure (CNII) that need the top priorities on managing the cybersecurity risks. Information Theft; Information Manipulation; Cyber Attack; and Identity Theft normally will jeopardized confidentiality, integrity and availability of the information that could lead to National Defense and Security. Another Critical National Information Infrastructure (CNII) sector is Banking and Finance. In banking and finance sector, numerous banking transaction every day involves billions of user bank account around the globe via online platform also highly exposed to cybersecurity risks. Cybersecurity Risks such Identity Theft could allows unauthorized access into personal user bank account and conducts illegal money transfer. Another, equally critical, sector that is now fully integrated with cyberspace is telecommunications. Telecommunications and IT are extensively employed for computerised control and supervision of sectors like power, nuclear energy, gas pipelines, etc., which are generally not connected to the internet, but are still vulnerable to malware attacks [25]. For that reason, Information and Communication sector need to give priorities in handling cybersecurity risks.

Cybersecurity risk is currently becoming serious issues in digital social media due to the increasing number of social media population growth. The spectrum of the risks are really wide and unpredictable. Cybersecurity risk caused by common risk factors, which is threats and vulnerability of information in social media. Social media allows social engineer use the psychological manipulation of people into performing actions confidential information for the purpose of information gathering, fraud or system access [15, 26–28]. Digital Social Media becomes the source of information for Social Engineer to capture and harvest the useful information for the purpose of the cyber attack.

Online Social Media might highly contribute to cybersecurity risks on Critical Information Infrastructure need to be identified and measure in order to understand the level of severity for each of them so that will be manage effectively. The capability of Online Social Media act as communication platform among cyber community, it's could also become a phishing pond for cyberwarfare and cybercrimes. For extreme cases, the impact of the cyberwarfare and cybecrime might cause human personal security, safety and psychological impact in nature.

4 Methodology

A study using questionnaire survey was applied in this research. Five-Point-Likert-Scale was used to measure the severity level of online social media cybersecurity risk on Critical National Information Infrastructure (CNII). Both primary and secondary data were used in order to accomplish this research objective. Cybersecurity risk factors for Malaysian social media digital users and cyber community as described in previous section were used to determine its risk severity on Critical National Information Infrastructure.

The research model in Fig. 1 is built based on the combination of several past literatures instead of a single research model. The research model discussed the cybersecurity risk factors in digital social media. Eighteen (18) cybersecurity risk factors were used in the research to determine their ranking based on risk criticalness in Digital Social Media directly affected the Critical National Information Infrastructure.

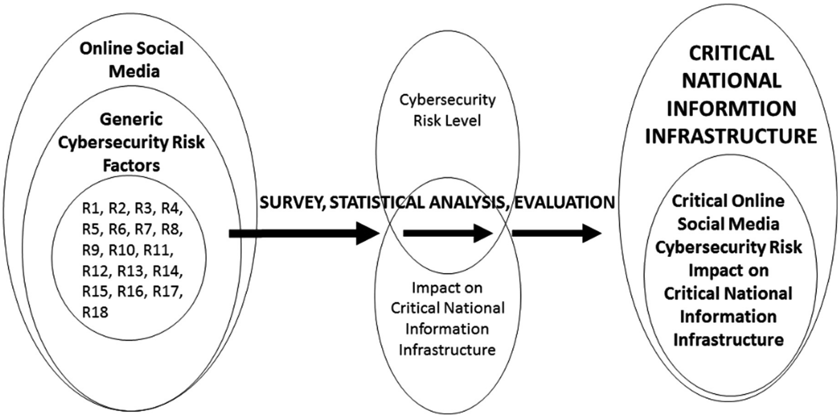
Online Social Media
Generic Cybersecurity Risk Factors
R1, R2, R3, R4, R5, R6, R7, R8, R9, R10, R11, R12, R13, R14, R15, R16, R17, R18
SURVEY, STATISTICAL ANALYSIS, EVALUATION
Cybersecurity Risk Level
Impact on Critical National Information Infrastructure
CRITICAL NATIONAL INFORMTION INFRASTRUCTURE
Critical Online Social Media Cybersecurity Risk Impact on Critical National Information Infrastructure

Fig. 1 Research analysis model

5 Results, Discussions and Findings

Data were collected from various private, government agencies and practitioners for the study. An appropriate statistical analysis used to analyze the results in order to conclude the findings.

5.1 Respondent's Demographic Profiles

Respondent's demographic profile examined were respondent's personal gender, age, professional experiences, organizational sectors and their industrial involvements. Most of them are the professional and senior executives from various organization and institutions in Malaysia. Therefore, the analysis shows that most of the respondent were consider as appropriate professionals that possess sufficient experience to response to the entire question trustfully and accurately. Table 1 summarized the demographic profiles of respondents involved in the study.

5.2 Reliability Test: Cronbach's Alpha Coefficient

Cronbach's Alpha Coefficient was used to test the survey item's reliability. A coefficient value which is closer to "1" is required. Cronbach Alpha value for Cybersecurity risks impact on critical national infrastructure, 0.977 are high. Since the value of reliability test more then 0.7, its considered as reliable. The value 0.7 used as a benchmark value of reliability test by others the researchers [29, 30] the scale for these construct were considered to exhibit an acceptable reliability. Table 2, briefly describes result of the reliability test.

Table 1 Respondent's demographic profile

	Frequency	Percentage (%)
Respondent's gender		
Male	18	54.5
Female	14	42.4
Respondent's age		
>50 years	3	9.1
46–50 years	2	6.1
41–45 years	6	18.2
36–40 years	6	18.2
31–35 years	8	24.2
26–30 years	7	21.2
Years of working experience		
>20 years	6	18.2
15–20 years	11	33.3
11–14 years	2	6.1
6–10 years	5	15.2
≤5 years	9	27.2
Years of ICT security experience		
>6 years	7	21.2
4–6 years	5	15.2
1–3 years	14	42.4
<1 year	7	21.2
Organizational sectors		
Private company	2	6.1
Government agencies	28	84.9
Government—link—company (GLC)	3	9.1
Industrial cluster		
Healthcare private	2	6.0
Healthcare government	1	3.0
Creative technology	2	6.0
Higher education	23	69.7
Information communication technology	2	6.0
Services	3	9.1

Table 2 Reliability test result: Cronbach's alpha value

Online social media cybersecurity risk factors	Items	Cronbach's alpha value	Total num. of respondents (N)
Critical national information infrastructure	18	0.977	33

5.3 Analysis Results: Online Social Media Cybersecurity Risk Factors Severity Level Impact on Critical National Information Infrastructure (CNII)

The highest mean in Table 3 represents the most severe impact of Online Social Media Cybersecurity Risk factors affected on Critical National Information Infrastructure while the lowest mean represents the least critical.

The highest mean in Table 3 represents the most severe impact of Online Social Media Cybersecurity Risk factors affected on Critical National Information Infrastructure while the lowest mean represents the least critical.

Analysis results from the study explore the severity level of Online Social Media Cybersecurity Risks factors on Critical National Information Infrastructure (CNII). Information Theft; Cyber Crime; and Cyber Attacks considered as the most critical cybersecurity risk factors from the study. Information Theft frequently cause by lack of cybersecurity awareness among Online Social Media users. Most of them usually not configure the security setting carefully for their social media account. As a results, personal confidential data, such files and photos could be at risk on

Table 3 Result: mean score ranking for critical cybersecurity risks severity level impact on critical national information infrastructure (CNII)

Online social media cybersecurity risk factors	Severity level impact on critical national information infrastructure (CNII)		
	Mean	Std. deviation	No. rank
Identity theft	3.59	1.073	7
Information manipulation[a]	3.72	1.023	3
Cyber assault/bullying	3.53	1.047	9
Advanced persistence threats[a]	3.72	0.958	3
Information theft[a]	3.78	0.941	1
Cyber crime[a]	3.78	0.906	1
Insider[a]	3.66	0.971	5
Espionage	3.56	0.914	8
Cyber attacks[a]	3.78	0.832	1
Transactional[a]	3.69	0.859	4
Attack of the software	3.53	1.047	9
Terrorisms	3.56	0.982	8
Phishing pond[a]	3.66	0.865	5
Privacy violation[a]	3.69	0.896	4
Risk of losing the legal battle	3.59	1.012	7
Corporate espionage	3.63	0.942	6
Viruses and malware[a]	3.72	0.888	3
Productivity loss[a]	3.75	0.880	2

[a] Top 5 Critical Social Media Cybersecurity Risks on CNII

information theft activities. Leakages of confidentiality data an information could lead to more Cybercrime and Cyber attack incidents that also associated to 10 critical sectors of National Information Infrastructure. Therefore, severity levels discovered from the study might be use as indicator an preliminary study for strategic planning to mitigate critical cybersecurity risks and manage its impact on Critical National Information Infrastructure (CNII) efficiently.

The second Cybersecuity Risk Factors was Productivity Loss. This cybersecurity risk factor is caused by poor planning in business recovery plan and lack of contingency plan to manage the impact of the risks. For example, if the cybersecurity risk affected Critical Information Infrastructure (CNII) especially in Information and Telecommunication sector, it's directly affected the quality of service. Meanwhile, other associated cybersecurity risk factors also could give serious problem to organization because it may interrupt the entire business operation. Finally it's will affected the productivity of the organization performance.

The third critical threat risk factors were Information Manipulation; Advanced Persistence Threats; and Viruses and Malware. Consequently, the Information Manipulation; Advanced Persistence Threats; and Viruses and Malware might definitely contributes to the risk of ICT failures may give impact to the entire operation and information management processes in 10 critical sectors of National Information Infrastructure especially those are highly depend on ICT services. For example, if our utility bills records had been manipulated higher than what it's cost by hackers/Viruses/Malware, we need to pay the higher bills for that we not use. If the service provider did not overcome this cybersecurity risk, its give bad reputation to customer. As a result, ICT service failures could damage the service provider image and reputation. Furthermore, public security and safety of the citizen could also at risks due to these failures.

Other critical Cybersecurity Risk Factors were Privacy Violation; Phishing Pond; Insider; and Transactional Attacks. Online Social Media could be the best platform for the source of information including the confidential data. Frequently, most of the social media user did not realized, they actually sharing their confidential information and personal data while updating their status or posted messages in social media platform. This information leakage is a critical problem for Critical National Information Infrastructure, where security information must be carefully managed and organized.

Conversely, Attack of the Software; Cyber Assault/Bullying; Espionage; Terrorisms; Risk of Losing the legal Battle. represents the lowest severity level from the same study. Attack of the Software rated the least critical because current advanced security technology able to manage attack of the software effectively. In addition, trends of the cybersecurity attack had change, hackers now prefer to harvest personal confidential information rather to attack the software.

Second least critical cybersecurity risk factors are Cyber Assault/Bullying through Online Social Media platform. Social media allows social engineer use the psychological manipulation of people into performing actions confidential information for the purpose of information gathering, fraud or system access as well as

Cyber Assault/Bullying. This attack could affected one of the 10 critical sector of information infrastructure which is public health dan safety of the social media user.

Third least critical cybersecurity risk factors are Espionage, the practice of spying or of using spies, typically by governments to obtain political and military information. Espionage provide information as to anyone who need the valuable information. Espionage easily capture these valuable information though Online Social Media platform because most of the user share almost all of their information, activities, location, etc. including their personal confidential data.

Even these cybersecurity risk factors considered as least critical affected the Critical National Information Infrastructure, special concern still needed to ensure the sustainability of the businesses and services.

In general, results of the analysis shows that, similar cybersecurity risk arise in Online Social Media and directly affected to the security of Critical National Information Infrastructure (CNII) but then the severity level were differently discussed due to several factors that contribute to the risks.

6 Conclusion and Future Directions

The existence of Online Social Media, had changed today knowledge society in every aspect of human life. It's changed personal lives, business activities, relational interaction, teaching and learning, communication and collaboration with various communities tremendously. However, if the sharing and disseminations of the confidential information via the social media could cause cybersecurity risks on Critical National Information Infrastructure (CNII). Analysis from this study shows some significant findings toward quantifying the severity level of cybersecurity risk factors on Critical National Information Infrastructure (CNII). Result of the analysis used as basis to prioritize the ranking of critical cybersecurity risk on Critical National Information Infrastructure.

The research finding discovered the top 5 most critical cybersecurity risk impact on Critical National Information Infrastructure (CNII) are Information Theft; Cyber Attacks; Cyber Crime; Information Manipulation; Productivity Loss. The findings indicates the similar nature of cybersecurity risk is critical. The human factors still considered the weakest link in cybersecurity incident on Critical National Information Infrastructure (CNII). Contrariwise, this article also highlight top 5 least critical cybersecurity risks impact on Critical National Information Infrastructure (CNII) which are Attack of the Software; Cyber Assault/Bullying; Espionage; Terrorisms; Risk of Losing the legal Battle.

Eventually, the findings possibly will provide an empirical evidences for the improvement to practitioner and technology implementer. Through the findings, experts, management and practitioners would be able to identify critical cybersecurity risk and address them more effective in order to minimize its related impact on Critical National Information Infrastructure (CNII) sectors. The findings through this study could also lead to the expansion of new knowledge and future discoveries.

References

1. Tang, Q., Gu, B., Whinston, A.B.: Content contribution for revenue sharing and reputation in social media: a dynamic structural model. J. Manag. Inf. Syst. **29**(2), 41–76 (2012)
2. Ngai, E.W.T., Tao, S.S.C., Moon, K.K.L.: Social media research: theories, constructs, and conceptual frameworks. Int. J. Inf. Manag. **35**, 33–34 (2015)
3. Kaplan, A.M., Haenlein, M.: Users of the world, unite! The challenges and opportunities of Social Media. Bus. Horiz. **53**(1), 59–68 (2010)
4. Jacka, J.M., Scott, P.R.: Auditing social media: a governance and risk guide. Wiley, Hoboken (2011)
5. Merriam-Webster Dictionary—Social Media. http://www.merriam-webster.com/dictionary/social%20media
6. Colliander, J., Dahlén, M.: Following the fashionable friend: the power of social media. J. Advertising Res. **51**(1), 313–320 (2011)
7. Hanna, R., Rohm, A., Crittenden, V.L.: We're all connected: the power of the social media ecosystem. Bus. Horiz. **54**(3), 265–273 (2011)
8. Hinson, G.: Top information security risk for 2008: information security risk. In: CISSP Forum, pp. 2–5, 2008
9. ISO/IEC 27000:2009 (E): Information technology—security techniques—information security management systems—overview and vocabulary. ISO/IEC (2009)
10. Best Practices in Social Networking Sites. Cyber Security Malaysia, 2011
11. Gasser, M.: Building a Secure Computer System (PDF), p. 3. Van Nostrand Reinhold, New York (1988). ISBN 0-442-23022-2
12. Online Source: Oxford English Dictionary online. Oxford University Press. Sept 2007. Archived from the original on 2012-07-08. Retrieved 27 Sept 2010
13. Online Source: Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield. Law.duke.edu. Retrieved 6 Feb 2016
14. Anderson, R.J.: Security engineering: a guide to building dependable distributed systems, 2nd edn, p. 1040. Wiley, Indianapolis, IN. ISBN 978-0-470-06852-6 (Chap. 2, p. 17)
15. Greavu-Şerban, V., Şerban, O.: Social engineering a general approach. Inf. Economica J. **18** (2), 2014 (2014)
16. Willison, R.: Understanding the perpetration of employee computer crime in the organisational context (PDF). Inf. Organ. **16**, 304–324 (2006)
17. Online Source: Blitz, J.: Security: a huge challenge from China, Russia and organised crime. Financial Times, 1 Nov 2011. Retrieved 6 Feb 2016
18. Understanding Information Infrastructure. http://heim.ifi.uio.no/~oleha/Publications/bok.pdf
19. National Cyber Security Policy-2013: Department of Electronics & Information Technology, Government of India. http://deity.gov.in/content/national-cyber-security-policy-2013-1
20. Amid spying saga, India unveils cyber security policy. Times of India. INDIA. http://timesofindia.indiatimes.com/tech/enterprise-it/security/Amid-spying-saga-India-unveils-cyber-security-policy/articleshow/20885499.cms?referral=PM
21. National Cyber Security Policy 2013: An Assessment. Institute for Defence Studies and Analyses. http://www.idsa.in/idsacomments/NationalCyberSecurityPolicy2013_stomar_260813
22. For a unified cyber and telecom security policy. The Economic Times. http://articles.economictimes.indiatimes.com/2013-09-24/news/42361275_1_national-information-board-national-cyber-security-policy-state-of-the-art-security-lab
23. Critical National Information Infrastructure. http://cnii.cybersecurity.my/main/about.html
24. Cybersecurity Definition. http://whatis.techtarget.com/definition/cybersecurity
25. For a unified cyber and telecom security policy. http://articles.economictimes.indiatimes.com
26. Wikipedia, The free encyclopedia, Social Engineering. http://en.wikipedia.org
27. Anderson, R.J.: Security engineering: a guide to building dependable distributed systems, 2nd edn, p. 1040. Wiley, Indianapolis, IN (2008). ISBN 978-0-470-06852-6 (Chap. 2, p. 17)

28. Irani, D.: Reverse Social Engineering Attacks in Online Social Networks. https://en.wikipedia.org/wiki/Social_engineering_(security)
29. Khidzir, N.Z., Arshad, N.H., Mohamed, A.: Information security risk factors: critical threats and vulnerabilities in ICT outsourcing. In: Proceedings of International Conference on Information Retrieval and Knowledge Management (CAMP'10), 2010, pp. 194–199 [10]
30. Rahim, N.N, Khidzir, N.Z., Yusof, A.M., Daud, K.A.M.: Towards a conceptual framework of animated infographics in an islamic context. In: Proceedings of 1st International Islamic Heritage Conference, 2015, pp. 38–48