Cybersecurity Readiness of E-tail Organisations: A Technical Perspective

Mahmood Hussain Shah, Raza Muhammad and Nisreen Ameen

[1] Coventry University, School of Strategy and Leadership, Coventry, United Kingdom
[2] Shah Abdul Latif University, Department of Mathematics, Khairpur, Pakistan
[3] Royal Holloway, University of London, School of Business and Management, London, United Kingdom

Abstract. Cybersecurity readiness is a challenging issue for online retail businesses which are losing billions of dollars due to cyber-crimes and a lack of readiness to manage these. Therefore, research into cybersecurity readiness in the online retail industry is needed. Technical tools are the foremost measures of defence against these attacks. This study investigates cybersecurity readiness from the technical perspective in some UK online retailers. This research adopted a qualitative case study approach with semi-structured interviews for collecting data. A total of 15 interviews were conducted with an online retail company's staff and management who had responsibility for managing cybersecurity. A thematic analysis method was used to analyse the qualitative data. The research findings show that the company is facing internal and external threats to their information systems and their technical defences are not very effective at present. The company should consider investing more resources in the technical controls to prevent these attacks.

Keywords: Cybersecurity; Technical Readiness; Organisational Readiness; Network Security; Cyber Threats and Risks.

1. Introduction

Cybersecurity has received significant attention from researchers and professionals. It has become an integral part of business activities in all organisations regardless of their size and nature and has become particularly important for online businesses. Cybersecurity readiness can be achieved by implementing a resilient culture against cyber related threats and attacks. This culture would be useful for organisations to mitigate the impact of cyber-attacks. However, these businesses are facing cybersecurity threats/attacks from both internal and external sources [1]. Cyber threats/attacks and frauds are increasing and posing many challenges for online organisations. These challenges include externals/ internals threats accidental damage and technical/organisational weaknesses.

Cyber threats include identity theft [2] and unauthorised access to an organisational network [3]. Denial of Service (DoS) attacks, malicious insiders, web-based attacks [4], human error [3], phishing emails and inadequate security monitoring [5] are also documented threats. There are some reasons which contribute to the success of these attacks, for example, preventative equipment failures [6], lack of technical awareness [7], unauthorised access [3] and malicious employees [4]. Some basic security controls such as encryption, anti-virus software, firewalls and intrusion detection systems (IDS) suggested by Sen, Ahmed, and Islam (2015) [8] could be used to prevent cyber-attacks. Unified Threat Management Systems (UTMS) provide more security to the network layer, hardware and software than standard security methods [9]. Secure authentication and authorisation systems are useful in preventing ID theft [10]. Regular assessment of security controls and monitoring of internal and external security systems may reduce the risk of cyber-attacks [11].

The aim of this research is to investigate the cybersecurity readiness, from a technical perspective, in an online retail organization, to assess how resilient its security infrastructure has been built to mitigate cyber-attacks. To achieve this aim, a qualitative case study was conducted and a total of 15 semi-structured interviews were conducted at an E-tail company in the UK. The semi-structured interviews provided an opportunity for face-to-face interactions with managers and other relevant staff. Additionally, policy documents were utilised in order to better understand the security processes in the company. Collected data was analysed using thematic analysis.

2. Literature Review

Cybersecurity readiness includes security policies, processes and procedures that are employed in the organisation to manage cyber threats. Furthermore, a review of cybersecurity readiness includes examinations of security functions, to check whether these functions operate in line with relevant policies, standards or procedures [12]. The importance of cybersecurity readiness has been increasingly recognised worldwide. Many leading countries have invested in their cybersecurity and have published official strategy documents for their cybersecurity; these include USA, UK, Canada, Australia, Japan, Germany and Russia [13].

Cybersecurity breaches are becoming increasingly common against companies regardless of their size and nature [14]. Cyber-attacks are malicious acts usually originating from an anonymous source that either steals, alters or destroys a specified target by hacking into a susceptible system. According to Uma & Padmavathi (2013) [15], several dimensions of cyber-attacks can be found in existing literature, but the primary objective of such attacks is to compromise the confidentiality, integrity and availability of information resources. These cyber-attacks tend to be successful due to weaknesses in technical infrastructure [16]. Due to a lack technical awareness, people become victims of cyber-attacks [7]. Therefore, this research focuses on cybersecurity readiness in the technical perspective to aid the online retail company in mitigating against potential cyber risk.

With the advancement in the technology, new methods of cyber-attacks are also emerging [14]. It is the responsibility of management to perform risk analyses and highlight flaws and vulnerabilities in the information systems, as neglecting these tasks can increase the likelihood of successful cybersecurity attacks. Therefore, online retail organisations must maintain update infrastructure to reduce the impacts of cyber-attacks in the organisation. Ultimately, these attacks affect organisations in the form of significant financial losses and reputational damage.

There are many technical threats that are possible reasons for cybersecurity breaches in online retail organisations. These include: Malware, Spam, Phishing, Spear-Phishing Attack, Denial of Service (DoS) attack, Distributed Denial of Service (DDoS), Man in Middle Attack, Hacking, Social Engineering, Spoofing, Keylogging, Cookies, Backdoor Trojan, SQL Injection and Identify Theft.

Impact of Cyber-attacks in Online Retail Organisations

Cybersecurity threats are a growing concern for online retail organisations. Organisations considered cyber-attacks to be the biggest threat to businesses. A recent study by Hui, Kim, and Wang (2017) [17] indicated that many DDOS attacks targeted banks (24%), telecommunications companies (23%) and financial services organizations (20%), indicating they were likely financially motivated. Another survey conducted by the PWC (2018) [18] indicates that the average financial cost of cybersecurity incidents (including costs relating to business operations and data) is £857,000. The same report also pointed out that UK organisations are more reluctant in combating against cyber-attacks than peer organisations in the other countries.

Countermeasures

The above discussion was about cybersecurity threats and attacks that affect online businesses in various forms. Effective counter measures are needed to prevent cybersecurity threats from materialising. There are several factors such as technical, organisational and human which increase the success rate of these attacks, for example, Uma and Padmavathi (2013) [15] state that there is a lack of proper understanding and technical awareness of the nature of cyber-attacks. By implementing security measures and controls, companies can help mitigate against these attacks.

Legitimate antivirus or endpoint security software along with user awareness regarding threats posed by clicking on suspicious links would be useful in mitigating cyber attacks. Organisations also use anti-spam software to limit the spam attacks, coupled with other countermeasures such as two factor authentication, web application scans, firewalls, access control, encryption and unified threat management appliances. However, the focus of this study is only cybersecurity readiness from a technical perspective and this can be achieved by proper implementation of technical controls to safeguard organisational infrastructure to mitigate the potential cyber-attacks.

3. Methodology

This study employs a qualitative case study approach, and focuses predominately on the perspectives conveyed by respondents, for instance, how they undertake their job roles to manage cybersecurity readiness in the online retail organisation. This approach allows the investigator to study real life events and managerial processes and it examines an existing phenomenon in depth within its real life situation [19]. This case study has been carried out in close interaction with practitioners who deal with managerial situations, so this approach is suitable to create relevant knowledge [20].

Participant Selection and Data Gathering

The study takes a case study based approach, using semi-structured interviews as the primary data collection method. The interview questionnaire was designed with the help of existing literature relevant to the field of information security. A pilot study was conducted with 10 academic staff in the relevant area of study and as a result, some amendments were made to the interview questions according to their suggestions. Moreover, participants were selected on the basis of their job nature and experience in the management of online security in the online retail company in the UK. A total of 15 interviews were conducted with professionals including the IT Manager, Fraud Prevention Manager and members of the Network Security Team. Face-to-face interviews lasted around 45-60 minutes. All interviews were audio recorded in a hand-held device to be transcribed and analysed later..

Data Analysis

The semi-structured interviews were transcribed manually. Furthermore, The Nvivo software was also used for the categorisation and coding of themes. This software is useful in transcribing, grouping, and coding the data. The thematic analysis method used to analyse the semi-structured interviews was proposed by Braun and Clarke (2006) [21]. Transcribed interviews were analysed using the inductive thematic analysis. This technique provides a facility to identify a set of emergent topics in the data. Each theme was carefully developed based on the analysis of transcribed text from interviews.

4. Results and Discussions

For this research, we conducted case study research at one large organisation. For confidentiality reasons, the case company will be referred henceforth as Company A. Company A is a leading multi-brand online retailer in the UK and Ireland, selling thousands of different brands supplied by others as well as its own brand of retail goods. In this section, we bring together the various observations from the data collected using semi-structured interviews at Company A to manage cybersecurity readiness in the technical context. Cybersecurity readiness can be achieved by implementing the following security controls (themes) which emerged from the analysis of collected qualitative data.

a) Access Control and Authentication

Usernames and passwords are treated commonly as authentication, but it is not a secure form of authentication because anyone can use these details and gain easy access to the systems. It is difficult for systems to recognise whether the user who has accessed system is genuine or fraudulent. Company A has two-factor authentication system to prevent unauthorised access. However, two-factor authentication is not always a secure method as cyber-criminals can violate this [22]. To make the authentication system more effective, biometric authentication systems may be used, for example, voice recognition, facial recognition and fingerprint scanning [23]. Therefore, Company A may consider biometric authentication systems to prevent unauthorised access.

b) Information Communication Security (ICS)

ICS helps to secure electronic communication amongst staff, third parties and customers inside and outside the company. Company A encrypts the data of customers and employees when sending it to third parties and registered post is used to send hard copies of data. Using encryption for sending and receiving information is useful for a company because it prevents modification and keeps data in its original form. This encryption method has a weakness as it does not cover the recipient of any data, as this would need Point-to-Point Encryption (P2PE). Therefore, Company A could P2PE to secure its communication channels more effectively [24]. Moreover, Public Key Infrastructure (PKI) digital signatures and Secure Sockets Layer (SSL) etc. are useful in preventing cybersecurity attacks [25]. Therefore, the company may use these for enhancing cybersecurity infrastructure.

c) Threat Management

Threat management is an essential component of the organisation's security process. Businesses that depend on ICT remain under threat from cyber-criminals whose motive is to steal sensitive information by infiltrating systems in different ways. Now, it is the responsibility of the organisation to manage such risks cost-effectively and minimise threats to their information systems.

Company A uses various security controls to minimise threats to information system infrastructure. Additionally, the company has professionals who constantly try to manage the security threats. However, some vulnerabilities still exist in these security controls for which Company A should assess regularly to manage security threats. This is also proposed by some researchers such as Taylor (2016) [11].

d) Network Security

Network security has a significant role in the information system security of online retail organisations because cyber-criminals attack the network to steal information. Cyber intrusions and attacks occur when unauthorised access is gained to networks, including theft of users' sensitive data, online economic fraud, website destruction, web application attacks and system penetration. Attackers exploit operating system vulnerabilities in web browsers, services and configurations, platform vulnerabilities in web applications, network device vulnerabilities, policy and personnel vulnerabilities in unauthorised devices [26]. Company A did face cyber-attacks, such as denial of service attacks, because of weaknesses in the network. However, encryption, anti-virus, firewalls, Intrusion Detection Systems (IDS) are useful in preventing cyber-attacks [8]. Therefore, the company should configure its firewalls to prevent denial of service attacks on the network. Firewalls are useful in preventing unauthorised access to the network and in blocking unwanted traffic into the company's network (Sen et al., 2015) [8]. A firewall is a shield that works against dangerous communications from disseminating across any network, either from the outside world into a local system, or from one part of a local network to another. It is a useful element in network access because it can prevent unauthorised access at the boundary of a network and infrastructure.

e) Network Monitoring

ICT enables business processes to operate electronically and provides facilities to conduct business activities more effectively and efficiently in the digital environment. The monitoring activities of ICT allow the company to detect vulnerabilities and respond to these appropriately by enhancing security controls. Despite such active monitoring systems, some information breaches still occur at Company A. Company A are monitoring activities inside the company and whenever unusual activity is found, they aim to resolve it immediately. The company also performs a test for vulnerabilities in its computing systems and try to fix it in the first instance. Further, the company has different teams whose work is to monitor the security processes of the company's infrastructure and prevent loopholes from being exploited. For network security, Unified Threat Management Systems (UTMS) provide more security to the network layer, hardware and software than standard detection methods because this is the combination of firewalls, pattern recognition and user authentication methods [9]. Therefore, Company A should use UTMS for effective security.

5. Conclusion

This paper presented the findings of the case study on cybersecurity readiness from a technical perspective, for instance, if ICT security and risk assessments are managed effectively; cybersecurity incidents in the organisation could be reduced. Therefore, the organisation should proactively asses their technical factors rather than only assessing these after an incident has occurred. A qualitative case study approach was adopted and 15 semi-structured interviews were conducted for data collection. The interviews were analysed using thematic analysis. The key areas of selected themes were discussed and confirmed by the managers and other staff members.

This research provides unique value through investigating the determinants of technical readiness. The study suggests that organisation readiness in the cybersecurity domain can be achieved by taking proactive measures such as ICT security and risk management. The results show that online organisations are lagging behind, especially in the effective implementation of up to date technical tools and measures. Although the case organisation has implemented some measures, there is still a need to explore their functionality within the organisational structure.

Like other studies, this research also has some limitations. Firstly, only a single case study was conducted in this research to evaluate the technical readiness. Secondly, only a qualitative case study approach was used for data collection. Therefore, there is a need to conduct multiple case studies to learn more about technical aspects of cybersecurity in other technical aspects, using both qualitative and quantitative methods. This study was conducted in the UK so repetition of this research in other countries would improve the research and extend results to compare and contrast the outcomes of online retailers.

References

[1] Manhart, M., Thalmann, S.: Protecting organizational knowledge: A structured literature review. Journal of Knowledge Management, **19**(2), 190-211 (2015)

[2] Humaidi, N., Balakrishnan, V.: Indirect effect of management support on users' compliance behaviour towards information security policies. Health Information Management Journal, **47**(1), 17-27 (2018)

[3] Da Veiga, A.: A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument. Paper presented at the Science and Information (SAI) Computing Conference, London, UK. July 13-15, 1006-1015 (2016)

[4] Clark, M., E. Harrell, C.: Unlike chess, everyone must continue playing after a cyber-attack. Journal of Investment Compliance, **14**(4), 5-12 (2013)

[5] Safa, N. S., Von Solms, R.: An information security knowledge-sharing model in organizations. Computers in Human Behavior, **57**(4), 442-451 (2016)

[6] Reason, J.: Managing the risks of organizational accidents. New York, Routledge (2016)

[7] Pieters, W., Hadžiosmanović, D., Dechesne, F.: Security-by-experiment: Lessons from responsible deployment in cyberspace. Science and Engineering Ethics, **22**(3), 831-850 (2016)

[8] Sen, P., Ahmed, A., Islam, R.: A study on e-commerce security issues and solutions. International Journal of Computer and Communication System Engineering, **2**(3), 425-430 (2015)

[9] Kent, C., Tanner, M., Kabanda, S.: How South African SMEs address cyber security: The case of web server logs and intrusion detection. Paper presented at the IEEE International Conference on Emerging Technologies and Innovative Business Practices for the Transformation of Societies (EmergiTech), Balaclava, Mauritius. Aug 3-6, 100-105. (2016)

[10] Sharma, A., Kansal, V., Tomar, R.: Location based services in M-commerce: Customer trust and transaction security issues. International Journal of Computer Science and Security (IJCSS), **9**(2), 11-21 (2015)

[11] Taylor, E.: Mobile payment technologies in retail: A review of potential benefits and risks. International Journal of Retail & Distribution Management, **44**(2), 159-177 (2016)

[12] Pereira, T., Santos, H.: A security audit framework to manage information system security. Global security, safety, and sustainability (9-18). Berlin, Germany, Springer (2010)

[13] Klimburg, A.: National cyber security framework manual. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence (2012)

[14] Waly, N., Tassabehji, R., Kamala, M.: Improving organisational information security management: The impact of training and awareness. Paper presented at the High Performance Computing and Communication & IEEE 9th International Conference on Embedded Software and Systems (HPCC-ICESS), Liverpool, UK. June 25-27, 1270-1275 (2012)

[15] Uma, M., Padmavathi, G.: A survey on various cyber attacks and their classification. IJ Network Security, **15**(5), 390-396 (2013)

[16] Shinde, P. S., Ardhapurkar, S. B.: Cyber security analysis using vulnerability assessment and penetration testing. Paper presented at the World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave), Coimbatore, India. 29 Feb.-1 March, 1-5 (2016)

[17] Hui, K., Kim, S. H., Wang, Q.: Cybercrime deterrence and international legislation: Evidence from distributed denial of service attacks. Mis Quarterly, **41**(2), 497-572 (2017)

[18] PWC: Revitalizing privacy and trust in a data-driven world: Key findings from the global state of information security® survey 2018 (2018). https://www.pwc.com/us/en/cybersecurity/assets/revitalizing-privacy-trust-in-data-driven-world.pdf. Accessed 11 Jan 2020.

[19] Yin, R. K.: Case study research: Design and methods. London, Sage publications Ltd (2014)

[20] Walsham, G.: Interpretive case studies in IS research: Nature and method. European Journal of Information Systems, **4**(2), 74-81 (1995)

[21] Braun, V., Clarke, V.: Using thematic analysis in psychology. Qualitative Research in Psychology, **3**(2), pp. 77-101 (2006)

[22] Srinivas, T., Vivek, G.. Cyber security: The state of the practice in public sector companies in India. Paper presented at the International Conference on Computer and Communications Technologies (ICCCT), Hyderabad, India. Dec 11-13, 1-5 (2014)

[23] Tan, F. T. C., Guo, Z., Cahalane, M., Cheng, D., Developing business analytic capabilities for combating e-commerce identity fraud: A study of trustev’s digital verification solution. Information & Management, **53**(7), 878-891 (2016)

[24] Ann McGee, J., Ralph Byington, J.: Corporate identity theft: A growing risk. Journal of Corporate Accounting and Finance, **26**(5), 37-40 (2015)

[25] Ray, S., Biswas, G., Dasgupta, M.: Secure multi-purpose mobile-banking using elliptic curve cryptography. Wireless Personal Communications, **90**(3), 1331-1354 (2016)

[26] Zhao, J. J., Zhao, S. Y., Opportunities and threats: A security assessment of state e-government websites. Government Information Quarterly, **27**(1), 49-56 (2010)