A study of evolving trends in cybersecurity risk

Shakir Abdulla M Barnawi

Email ID: Shaker939@gmail.com

Abstract

Over the last three decades, Information Technology (IT) has become indispensable thing for every walk of life and the concept of cybersecurity has existed *inter-alia.* In usual sense, Cybersecurity can be defined as the practice of safeguarding computer networks, system and files from digital threats which are emerging from inside or outside of the organization. In its 2022 study report “Cybersecurity solutions for a riskier world”, Thought Lab (2022) has analyzed in its 2022 benchmarking study that 1200 large organizations across 14 different sectors and 16 countries have spent $125.2 billion towards cybersecurity measures. Even with such efforts, any organization can’t say itself foolproof from common cyber-attacks, viz. phishing, network intrusion, unintentional disclosures, system misconfiguration, loss of data/devices etc. Now-a-days, the cybercriminals have become more prolific and the cybersecurity executives anticipate an increase in attacks from social engineering and ransomware. These attacks might target the weak spots which are possibly caused by software misconfiguration, human-error, poor maintenance, unknown assets etc. Thus, this study paper strives to analyze some of the most contemporary risk trends, which are evolving in cybersecurity landscape and further, to pinpoint some of the effective solutions to combat such anticipated risk factors.

Keywords: Information Technology, Cybersecurity, Cybersecurity Risks, Trends and Solutions, Social Engineering, Ransomware

Introduction

In modern times, cybersecurity measures are marred with daunting challenges emanating out of asymmetric nature of threats. Organizations keep on allocating higher and higher budgets to combat cyber threats but the later continue to grow exponentially. Bone, J. (2016) has described this phenomenon as “Cyber Paradox” which has turned out to be an entrenched battle for security professionals in defending against an increasingly sophisticated adversary that, to date, has adapted faster than defensive measures to prevent loss of data or access to sensitive information. He, further, goes on to state that the human-machine interaction is the greatest threat in cyber space yet very few, if any, security professionals are well versed in strategies to close the gap caused by adopting less effective conventional security measures to combat cybersecurity threats. Rees, et al. (2011) observed that security countermeasures help ensure the confidentiality, availability, and integrity of information systems by preventing or mitigating asset losses from Cybersecurity attacks. However, the uncertainty factor makes it difficult to assess the quantum of risk and further, to prescribe the exact countermeasure to be employed. It can also be held that the organizations are witnessing dynamic cybersecurity challenges simultaneously, with the emerging technologies which are employed with intent to increase efficiency of the services of those organizations. Cyber risk landscape is expanding in view of the use of emerging technologies which, in turn, are responsible for new types of malwares, phishing tools etc. Apart from these established results, it is also important to discuss the psyche of the organization towards cybersecurity risks. Many of the organizations still employ bottomup approach to deal with these risks and employing more scientific approaches is still in nascent stage. Alberts & Dorofee (2003) have observed that even though the highest frequency of cyber-attacks in an organization comes from outside, there are indicators that the most costly attacks come from inside. Thus, cybersecurity risks are attributed to both internal and external threats and these multifaceted vulnerabilities keep these risk trends ever evolving.

Thus, in view of above discussion, it is pertinent to identify the contemporary trends in cybersecurity risk, knowing that these risk factors ought to be handled in very proactive manner, as the very existence of organizations, these days, are much dependant on effective management of these risks. Accordingly, this review paper strives to discuss the evolving trends in cybersecurity risk and effective management thereof for viable functioning of the organizations.

Methodology

This study paper is a result of genuine thought process and analysis of the readily available research literature on information-security / cybersecurity risk. Further, some specific journals of established international agencies and comparative statistics have been assessed in order to accentuate discussion and findings during the review work.

Findings and Discussion

We are now living in a world where the internet and digitally dependent operations are fast developing and changing. With the surge of “Internet of Things (IoT)”, individual IoT devices, such as Smart TVs, Cellphones, Voice assistants etc. which are connected to internet or other networks, offer access points to hackers. These hackers, in turn, access individuals’ Wi-Fi credentials and valuable personal data and they are well versed in gaining entry into a network through personal devices. Chertoff, M. (2018) has cautioned about a pervasive exposure of individuals’ personal information, which has become increasingly vulnerable to cyber-attacks. Further, cyber attackers are well versed in gaining entry into a network through personal devices. Similarly, the corporations and governments also remain at constant risk due to numerous sophisticated developments, viz. phishing, malwares, ML & AI, cryptocurrency etc. The shortage of cybersecurity professionals also play a pivotal role in continuous evolving of such risks. Dr. Michelle Moore of University of San Diego has outlined in a report titled “Top Cybersecurity Threats in 2022” that the companies and the governments have struggled to hire enough qualified professionals to safeguard against the growing threats. She has further expressed that by 2021, the industry might have faced shortage of around 3.5 million cybersecurity professionals and this trend is expected to continue in 2022 as well.

With this background, henceforth, it is pertinent to shift our attention towards some of the most evolving trends in cybersecurity risks and possible measures to handle those risks. In the age of COVID-19 pandemic, Work from home (WFH) has emerged as the topmost cause for cybersecurity risk. Borkovich & Skovira (2020) have asserted that the humongous increase in successful cyber-attacks is directly attributed to the number of people working remotely or telecommunicating due to the invisible threat of COVID-19. Human factor is consistently blamed as security’s weakest link due to behavioral, social, and cultural vulnerabilities (Angwin, 2014; Garrett & Danziger, 2008). In WFH environment, it is common to have greater data access or more administrative rights than required. These setups are less protected than the centralized offices, which have more secure firewalls, router and access managed by committed IT team. Thus, it becomes easy for cybercriminals to take ulterior advantage of WFH facilities. Thus, in order to mitigate cybersecurity risks in WFH facilities, one should resort to secure the home Wi-Fi by employing antivirus and internet security softwares. Further, the users should be made to work in robust and authenticated Virtual Private Network (VPN) of the company. Encryption method for VPN access can again be enhanced, e.g. by upgrading to L2TP (Layer 2 Tunneling Protocol) from the usual PPTP (Point-to-Point Tunneling Protocol). Using strong and secure passwords and enhance 2-factor authentication are some other methods to mitigate cybersecurity risks in WFH environments.

Lee (2020) has stressed upon cybersecurity as one of the most important areas of Internet of Things (IoT). It is a well-known fact that IoT risk has direct bearing over organizations' assets and privacy concerns. Security management of the IoT is challenging due to the dynamic and transient nature of the connection between devices (Atzori, et al. (2010)). Organizations have encountered numerous issues related to business operations, finance, compliance etc. due to increasing cybersecurity attacks on IoT systems. A PwC survey has reported that IoT-based threats will become more widespread and impactful, and senior management will need to pay more attention to IoT-related risks when developing organization-level cyber risk management. Aldmour, et al. (2019) expressed concerns that the existing risk assessment methods are not appropriate for dynamic systems such as IoT. Further, a Business Insider (2022) report has estimated that there will be 64 billion IoT devices installed around the word by 2026 and this will be immensely helped by the increasing trend of remote working. Thus, given the wider implication of IoT, organizations need to implement appropriate IoT infrastructure in place to combat cybersecurity risk emanating out of IoT objects. Karale, A. (2021) has suggested a five-layered IoT infrastructure and he has further emphasized on security, ethics, privacy and laws in order to combat IoT cybersecurity challenges.

Further, the lust for easy finances and intricacies of IT operations in the wake of COVID-19 pandemic has given rise to new kind of Ransomware risk in cybersecurity arena. Reshmi (2021) has stated that ransomware is the most predominant cyber threat in digital infrastructure as it imposes a high financial burden on the organizations. It has affected a broad spectrum of industries like transport, telecommunications, financial companies, public law enforcement and health services. Ransomware either encrypts the files or locks the devices and demands the organization to pay ransom to retrieve the access (Hansman & Hunt, 2005). These attacks have become more sophisticated with advancement in machine learning and dark web technologies. System vulnerabilities, such as using outdated softwares, non-patched browsers / operating systems, obsolete devices etc., add to the ransomware menace. Further, the hackers demand to pay in cryptocurrencies, which are very difficult to trace. In 2020, the first ransomware induced death was reported in Germany, wherein cyber-attackers locked a hospital out of its systems and a woman in need of urgent care succumbed. Some of the possible safeguarding against ransomware attacks can be enumerated as follows:-

- Not to click the unsafe links.
- Don't open the suspicious email attachments.
- Continuous updating of programs and operating systems.
- Don't download from unknown sources or use unknown USB drives.
- Always prefer VPN services over public Wi-Fi networks.

Social engineering attacks have emerged as yet another cybersecurity risk component with the advent of remote work culture. Salahdine & Kaabouch (2019) have asserted that social engineering is one of the biggest challenges facing network security because it exploits the natural human tendency to trust. These attacks aim at tricking individuals or enterprises into accomplishing actions that benefit attackers or providing them with sensitive data such as social security number, health records, and passwords. The worst part with these attacks is they can be detected but not stopped, hence these are being perceived as the biggest threats in the face of cybersecurity. Mouton, et al. (2016) identified that these attacks follow common pattern which involves four phases: (1) collect information about the target; (2) develop relationship with the target; (3) exploit the available information and execute the attack; and (4) exit with no traces. These attacks can be classified among technical, social and physical categories and phishing, baiting, pretexting, tailgating, impersonation, shoulder surfing, pharming, vishing, SMSishing etc. are some prominent examples of social engineering. Osuagwu, et al. (2015) have expressed that social engineering attacks are very significant security risks and addressing these attacks should be part of the risk management strategy of companies and organizations. Companies should make a commitment to the security awareness culture among their employees. In order to detect and prevent these attacks, a number of techniques have been proposed. A list of defense procedures for social-engineering attacks include: encouraging security education and training, increasing social awareness of social-engineering attacks, providing the required tools to detect and avoid these attacks, learning how to keep confidential information safe, reporting any suspected activity to the security service, organizing security orientations for new employees, and advertising attacks' risks to all employees by forwarding sensitization emails and known fraudulent emails (Foozy, et al. (2011)).

The last decade has witnessed phenomenal rise of Artificial Intelligence (AI) and Machine Learning (ML). Some of the key advantages of these new technologies are building automated security systems, natural language processing, analyzing massive quantity of data, automatic threat detection etc. However the recent developments suggest that even these cutting edge technologies are not absolved of risks (AI & ML risks). Tang, et al. (2017) have elaborated that complex big data systems in modern organizations are progressively becoming attack targets by existing and emerging threat agents. As per Rawat, et al. (2019), the ability to gather information from large volumes of data has become an issue of relative importance and the growing value of data has made big data a high value target. For AI/ML systems, the big data and the data model are two critical assets which are vulnerable to system manipulations, data corruption / poisoning and data privacy concerns. Towards mitigation of such AI & ML risks, concerning Big Data, it is noteworthy to mention Kshetri (2014), who has vouched that security and privacy issues associated with big data have attained at least some degree of institutionalization in industrialized countries and though many developing countries currently have no regulatory safeguards in place, but big data related issues are being considered in a setting of nascent institutionalization. Apparently, the companies are very much concerned about big data security and the way forward for managing this risk is to have right information, commitment towards data integrity, skilled resources and adaptive strategies.

While concluding, it is pertinent to discuss Mobile threats as yet another modern cybersecurity concern, which is gaining momentum in the era of accelerated remote working. These threats may include specialized spyware, SMS spam, DDoS (Distributed Denial of Service), exploiting security vulnerabilities within devices etc. Almaiah, et al. (2019) have rightly asserted that the most of cyber threats classifications are usually limited and based on one or two criteria in the classification process of threats, hence an exhaustible list of cyber threats on mobile devices and applications couldn't be presented in the existing frameworks. In the words of Weichbroth & Lysik (2020), communicating mobile security threats and best practices has become a central objective due to the ongoing discovery of new vulnerabilities of mobile devices. Implication of these risks encompasses IoT, network security, cloud security and other elements, viz. automated devices, wearable etc. Further, the mobile devices, based on a specific operating system, enable users to install a vast variety of applications, commonly referred to as "apps," from online sources called markets: Apple App Store, and Google Play (Guo, et al. (2019)). In the words of Mavoungou, et al. (2016), the aforementioned apps are the essence of smartphones, enriching their functionality and enhancing the everyday lives of their users. The app markets allow users to perform a quick search and installation of new apps, but at the same time, they are also a source of different kinds of malware disguised as normal apps. Nowadays, mobile devices are subject to a wide range of security challenges and malicious threats. Due to obvious oddities related with these types of threats, we can't claim a particular method, being apt, for mitigation. Stricter credentials for reinforcing sensitive data storage and ensuring additional security layers are few measures to look for while dealing with these risks.

Conclusion

Modern developments suggest that majority of the organizations have started considering cybersecurity as a business risk rather than simply a technical problem for IT. A Garter press release dated 21.06.2022 reported that by 2025, 60% of organizations will use cybersecurity risk as a primary determinant in conducting third-party transactions and business engagements and 30% of nation states will pass legislation that regulates ransomware payments, fines and negotiations, up from less than 1% in 2021.

In such a demanding scenario, a discussion on major cybersecurity risks is very significant in today's context. This study has strived to chart out some the most prominent cybersecurity threats which have evolved in modern times, especially in the wake of COVID-19 pandemic and simultaneously, some of the apt mitigation strategies for respective threats have also been outlined. This discussion has not covered exhaustive list of cybersecurity threats as these are very dynamic in nature and still evolving. Thus, cybersecurity risk domain requires exclusive study and research to gauge the implications and mitigation strategies for such risks.

References

Alberts, C. J., & Dorofee, A. J. (2003). *Managing information security risks: the OCTAVE approach*. Addison-Wesley Professional.

Aldmour, R., Burnap, P., & Lakoju, M. (2019). Risk assessment methods for converged IoT and SCADA systems: Review and recommendations.

A Look at examples of IoT devices and their business applications in 2022 report, available online: https://www.businessinsider.com/internet-of-things-devices-examples?r=US&IR=T last accessed on 29.11.2022.

Almaiah, M. A., Al-Zahrani, A., Almomani, O., & Alhwaitat, A. K. (2021). Classification of cyber security threats on mobile devices and applications. In *Artificial Intelligence and Blockchain for Future Cybersecurity Applications* (pp. 107-123). Springer, Cham.

Angwin, J. (2014). Dragnet nation: A quest for privacy, security, & freedom. New York: Times Books.

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer networks*, *54*(15), 2787-2805.

Bone, J. (2016). Cognitive Risk Framework for Cybersecurity: Bounded Rationality: Executive Summary: Part I. *EDPACS*, *54*(5), 1-11.

Borkovich, D. J., & Skovira, R. J. (2020). Working from home: Cybersecurity in the age of COVID-19. *Issues in Information Systems*, *21*(4).

Chertoff, M. (2018). *Exploding Data: Reclaiming Our Cyber Security in the Digital Age*. Atlantic Monthly Press.

Cybersecurity Solutions for a Riskier World (2022) report retrieved from https://thoughtlabgroup.com/cyber-solutions-riskier-world/ last accessed on 28.11.2022.

Foozy, C. F. M., Ahmad, R., Abdollah, M. F., Yusof, R., & Mas'ud, M. Z. (2011, November). Generic taxonomy of social engineering attack and defence mechanism for handheld computer study. In *Malaysian Technical Universities International Conference on Engineering & Technology, Batu Pahat, Johor*.

Garrett, R. K., & Danziger, J. N. (2008). On cyberslacking: Workplace status and personal Internet use at work. Cyberpsychology & Behavior, 11(3), 287-292.

Gartner Unveils the Top Eight Cybersecurity Predictions for 2022-23 report retrieved from https://www.gartner.com/en/newsroom/press-releases/2022-06-21-gartner-unveils-the-top-eight-cybersecurity-predictio last accessed on 30.11.2022.

Guo, B., Ouyang, Y., Guo, T., Cao, L., & Yu, Z. (2019). Enhancing mobile app user understanding and marketing with heterogeneous crowdsourced data: a review. *IEEE Access*, *7*, 68557-68571.

Hansman, S., & Hunt, R. (2005). A taxonomy of network and computer attacks. *Computers & Security*, *24*(1), 31-43.

Karale, A. (2021). Internet of Things.

Kshetri, N. (2014). The emerging role of Big Data in key development issues: Opportunities, challenges, and concerns. *Big Data & Society*, *1*(2), 2053951714564227.

Lee, I. (2020). Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management. *Future Internet*, *12*(9), 157.

Mavoungou, S., Kaddoum, G., Taha, M., & Matar, G. (2016). Survey on threats and attacks on mobile networks. *IEEE Access*, *4*, 4543-4572.

Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. *Computers & Security*, *59*, 186-209.

Osuagwu, E. U., Chukwudebe, G. A., Salihu, T., & Chukwudebe, V. N. (2015, November). Mitigating social engineering for improved cybersecurity. In *2015 International Conference on Cyberspace (CYBER-Abuja)* (pp. 91-100). IEEE.

PwC. Managing Emerging Risks from the Internet of Things. 2016. Available online: https://www.pwc.com/us/en/services/consulting/cybersecurity/library/broader-perspectives/managing-iot-risks.html last accessed on 29.11.2022.

Rees, L. P., Deane, J. K., Rakes, T. R., & Baker, W. H. (2011). Decision support for cybersecurity risk planning. *Decision Support Systems*, *51*(3), 493-505.

Rawat, D. B., Doku, R., & Garuba, M. (2019). Cybersecurity in big data era: From securing big data to data-driven security. *IEEE Transactions on Services Computing*, *14*(6), 2055-2072.

Reshmi, T. R. (2021). Information security breaches due to ransomware attacks-a systematic literature review. *International Journal of Information Management Data Insights*, *1*(2), 100013.

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet*, *11*(4), 89.

Tang, M., Alazab, M., & Luo, Y. (2017). Big data for cybersecurity: Vulnerability disclosure trends and dependencies. *IEEE Transactions on Big Data*, *5*(3), 317-329.

Top Cyber Threats in 2022 report by Michelle Moore, Ph.D., retrieved from https://onlinedegrees.sandiego.edu/top-cyber-security-threats/ last accessed on 29.11.2022.

Weichbroth, P., & Łysik, Ł. (2020). Mobile security: Threats and best practices. *Mobile Information Systems*, *2020*.