mPower tech: IT consultation services

Tyre F. Thompson

CYSE: 494 Cybersecurity entrepreneurship

June 21, 2023

Introduction

In today's interconnected digital landscape, cybersecurity has emerged as a paramount concern for individuals and organizations alike. While technological advancements have bolstered cybersecurity measures, the human factor remains a critical vulnerability. Cyber attacks often exploit human error, social engineering tactics, and lack of cybersecurity awareness, making it imperative to address this aspect comprehensively. This overview explores the problem of the human factor in cybersecurity and introduces mPower Tech, an innovative IT consultation service that seeks to empower individuals and organizations to mitigate this critical vulnerability. The increasing frequency and sophistication of cyber threats have highlighted the pressing need for effective cybersecurity strategies. While advancements in technology have brought about significant improvements in safeguarding digital assets, cybercriminals have adapted their tactics to exploit the weakest link in the security chain: humans. The human factor, encompassing the actions, behaviors, and decision-making of individuals within the digital ecosystem, has emerged as a primary target for cyber attackers.

Problem: The Human Factor in Cybersecurity The human factor poses a significant challenge to maintaining robust cybersecurity defenses. Despite technological advancements and sophisticated security systems, cyber attackers continue to exploit human vulnerabilities as an entry point. Employees may unintentionally click on phishing emails, fall for social engineering techniques, or neglect best cybersecurity practices, thereby compromising sensitive data and systems. Additionally, individuals often lack awareness of emerging threats, making them susceptible to cyber risks. Addressing this human factor is crucial to fortify cybersecurity measures effectively. The human factor in cybersecurity presents a multifaceted challenge that organizations must address to maintain robust defenses against cyber threats. Despite the

implementation of advanced technological solutions and sophisticated security systems, cyber attackers consistently target and exploit human vulnerabilities as an entry point into protected networks and systems. One common manifestation of the human factor is through social engineering tactics, which manipulate individuals' trust and emotions to deceive them into disclosing sensitive information or granting unauthorized access. Phishing attacks, for example, involve the use of fraudulent emails or messages that appear legitimate, tricking unsuspecting employees into clicking on malicious links or providing login credentials. These social engineering techniques capitalize on human psychology and the innate inclination to trust, making individuals susceptible to manipulation.

Overview of the Innovation: mPower Tech IT Consultation Service mPower Tech is an innovative IT consultation service that recognizes the paramount importance of addressing the human factor in cybersecurity. Their comprehensive approach focuses on empowering individuals and organizations through tailored solutions, awareness programs, and cutting-edge technologies. By combining technical expertise with a human-centric approach, mPower Tech aims to enhance cybersecurity resilience. mPower Tech's IT consultation service is built upon the foundation of deep expertise in cybersecurity. They understand the evolving landscape of cyber threats and recognize that effective cybersecurity strategies must extend beyond technical solutions. With this understanding, mPower Tech offers tailored solutions that are specifically designed to meet the unique needs and challenges faced by organizations in mitigating the human factor. Through thorough assessments, mPower Tech identifies vulnerabilities within an organization's cybersecurity infrastructure. This allows them to develop customized strategies and implement targeted mitigation measures that address the specific risks associated with human vulnerabilities. By taking a personalized approach, mPower Tech ensures that

organizations can effectively safeguard their critical assets and sensitive information from cyber attacks that exploit the human factor.

Tailored Solutions: mPower Tech recognizes that cybersecurity needs differ for each organization. Their IT consultation service provides customized solutions tailored to specific requirements, ensuring that vulnerabilities are effectively identified and addressed. This approach acknowledges the unique challenges faced by organizations, allowing for targeted mitigation strategies.

Awareness Programs: mPower Tech places great emphasis on cybersecurity education and awareness. They offer comprehensive training programs that educate individuals on the latest cyber threats, social engineering techniques, and best practices for maintaining robust cybersecurity hygiene. By promoting a culture of cybersecurity awareness, mPower Tech empowers individuals to make informed decisions and act as the first line of defense against cyber threats.

Cutting-Edge Technologies: mPower Tech leverages advanced technologies to enhance cybersecurity measures. They provide state-of-the-art tools, such as intrusion detection systems, threat intelligence platforms, and behavior analytics, to proactively identify and mitigate cyber risks. These technologies enable organizations to detect potential breaches, protect critical assets, and respond swiftly to emerging threats.

Collaborative Approach: mPower Tech adopts a collaborative approach, working closely with organizations to foster a cybersecurity culture. They engage stakeholders at all levels, encouraging open communication, knowledge sharing, and continuous improvement. By building strong partnerships, mPower Tech creates an environment that encourages active participation in cybersecurity practices, fostering collective responsibility.

Review:

The literature review delves into how business vulnerabilities affect cybersecurity by examining various studies conducted by researchers studying different aspects of vulnerabilities and their consequences. These studies contribute to understanding better how essential it is to secure digital data from cyber attacks. In Cavusoglu et al.s' (2004) research they analyze market reactions on announcements regarding digital security breaches looking at their financial impacts on breached firms' market value which varied among internet security developers. Furthermore Daengsi et al.s (2021) focus is on enhancing cybersecurity awareness among employees in various organizational departments regarding phishing attacks through comparative analysis identifying differences in awareness levels and susceptibility to cyber-attacks across different departments necessitating tailor-made training programs targeting specific departmental-specific cybersecurity awareness improvement.

Additionally, Gupta and Hammonds' (2013) comprehensive study identifies several factors influencing employees' information security awareness such as organizational culture, management support, training programs, and communication channels. Their findings emphasized the need for these variables promoting employee adequate cyber awareness behavior while providing critical insights on gaps existing literature identifies a necessity for further research assessing the effectiveness of cybersecurity interventions.

Overall, these academic studies are invaluable in understanding business vulnerabilities within the realm of Cybersecurity whilst mitigating risks aligning with mPowerTechs' objective toward enhancing organizational resilience. Using knowledge gleaned from these studies can help businesses navigate digital vulnerabilities effectively while adopting secure Cybersecurity practices by providing customized solutions and educational resources.

Best Practices, Etiquette, and Impacts of Attacks on Businesses

Persistent cyber threats targeting businesses are an ongoing issue increasingly affecting companies worldwide. Therefore adopting strategies that ensure appropriate manners are met throughout all aspects of operations has become more pressing than ever before. Research studies examine various approaches by assessing best practices for employee effectiveness when confronting common challenges associated with cybersecurity risks or incidents like those posed by phishing attacks. Kirlappos and Sasse (2013) suggest integrating security education on phishers, which has proven helpful during ongoing educational programs. Their research highlights the significance of enhancing user awareness and their grasp of this prevalent attack method.

In addition, Herath and Rao (2009) present a framework for promoting the compliance of security policies within corporate organizations. The study explores factors that can influence employees' adherence to such principles while assessing motivational mechanisms and deterrence strategies. Its findings underscore creating an environment that prioritizes measures aimed at motivating employees to comply with existing policies while at the same time considering punitive actions as reliable deterrents.

Lastly, Dhamija et al.'s research analyses psychological elements contributing to phishing attack success; they analyze deceptive design and social engineering tactics responsible for making individuals susceptible to such attacks. Their study concludes by emphasizing users' training regarding design improvements but is also advocating for technological countermeasures as essential methods towards mitigating the impact arising from successful phishing attacks. mPowerTech aligns with these academic studies by focusing on employee training, awareness development, security policy implementation, covering human factors in technology design

systems development - all relevant areas essential in identifying cybersecurity threats effectively through educational programs implemented throughout businesses worldwide effectively. Organizations must prioritize the integration of best practices alongside promoting cybersecurity awareness among employees to foster a culture of compliance. By doing so systematically across all organizational departments carefully choosing partners/vendors who shares similar values - those organizations will not only safeguard their critical resources but also earn unwavering loyalty from esteemed customers while bolstering their reputation in the marketplace.

Cybersecurity Frameworks:

Swar and Hossain (2020) conducted a systematic review to explore the relationship between organizational cybersecurity awareness and compliance. Their study identified factors such as individual behavior, organizational culture, and training programs that influence cybersecurity awareness, underlining the importance of fostering a culture of cyber safety in enhancing organizational practices. Hence, it is crucial for mPowerTech to develop continuous education and monitoring programs tailored towards enhancing organizational compliance.
On a similar note, Azmi, Tibben, and Win (2018) reviewed various cybersecurity frameworks to identify shared concepts' contextual relevance on various frameworks available in literature to enhance cyber defenses on an organizational level like NIST Cybersecurity Framework & ISO 27001. This study emphasized that aligning organizational efforts with recognized frameworks provides additional benefits in establishing an effective security strategy while promoting standardization across multiple sectors digitally impacted.

The National Institute of Standards and Technology (NIST) has developed the Framework for Improving Critical Infrastructure Cybersecurity; this framework represents an industry-standard approach towards safeguarding infrastructure against cyber threats by offering

five core functions: identifying risk management strategies continuously evolving across industries responding effectively by developing protective measures suited for the organization's unique needs.

mPowerTech can leverage insights from academic studies into practice by encouraging clients to adopt recognized frameworks, utilizing benefits accruing due to standardization it promotes while implementing tailored protective measures aligned with specific requirements effectively using insights from these studies specifically NIST Framework customized suitably as per client's requirement responding proactively towards creating resilient organizations aware of cyber risks adopting due diligence while meeting their obligations digitally safeguarding their assets effectually resulting reduced financial losses due to costly breaches impacting negatively as per experience across sectors today. The speaker kindly disputes the argument proposed. Citing its lack of factual support. Additionally. It seems evident that no effort has been made towards grasping a complete understanding of this issue.

Management and Risk Assessment

Organizations need an effective approach to manage critical digital threats associated with a robust cybersecurity mechanism. In this article. We explore three reliable sources that offer credible insights into better understanding cyber risk assessment and management particularly suited to small and medium sized enterprises (SMEs). According to Von Solms and Van Niekerk (2013) developing a holistic approach is crucial while devising security measures aligned with the intended organizational objectives. The researchers suggest taking people. Processes as well as technology into account when formulating risk management strategies related to required elements necessary for good practices against potential cyber risks. Incorporating these concepts into our tailored organizational risk assessments strengthens the

architecture of client specific cybersecurity strategies overall coping mechanisms adopted prevent any unexpected breach attempts. Sukumar et al. published a research paper in 2023 that provides more specialized insights into assessing potential cyber risks.

Their risk assessment approach incorporates criteria such as identifying vulnerable areas and threat severity while ensuring highly effective countermeasures at different organizational levels aligning seamlessly with NIST Framework. Our integration of professional opinions and other reliable sources enhances our overall capabilities to address cybersecurity threats more effectively taking into account the clients' requirements and contextual needs. We impart specialized approaches to benefit SMEs who can identify and address vulnerabilities associated with their given context promptly. Saving them from suffering significant financial losses or reputational harm.

Our approach includes selecting frameworks that are optimal for clients' contextual needs while also considering critical elements including technology processes as well as people that contribute to creating more effective digital security measures overall.

Problem Overview and Innovation as It Relates to Outside Fields

By drawing from various academic disciplines, a deeper understanding of the human element in cybersecurity can be achieved, and the potential of mPower Tech's IT Consultation Service can be fully appreciated.

Psychology: Psychology provides valuable insights into human behavior, cognition, and decision-making processes, which are crucial in understanding the human factor in cybersecurity. Courses in psychology can cover topics such as cognitive biases, social engineering, and user behavior. Understanding these psychological aspects helps identify why individuals may fall victim to cyber attacks or engage in risky online behavior. By incorporating

principles from psychology, mPower Tech's IT Consultation Service can design effective cybersecurity awareness programs, tailored training modules, and behavior-focused incident response strategies.

Human Factors Engineering: Human factors engineering focuses on the design and optimization of systems to enhance human performance, safety, and usability. This field explores the interaction between humans and technology, addressing ergonomics, cognitive workload, and user experience. Understanding human factors is critical in addressing the human element in cybersecurity, as it helps identify usability issues, design effective security interfaces, and create secure workflows. mPower Tech's IT Consultation Service can leverage principles from human factors engineering to develop user-centric cybersecurity solutions.

Organizational Behavior and Management: Courses in organizational behavior and management explore topics such as leadership, teamwork, and organizational culture. These areas have direct implications for cybersecurity, as organizations need to establish a security-oriented culture, ensure effective communication, and promote security awareness among employees. By understanding the dynamics of organizational behavior, mPower Tech's IT Consultation Service can collaborate with organizations to align cybersecurity initiatives with existing management practices and promote a secure work environment.

Legal and Ethical Considerations: Legal and ethical studies explore the moral and legal implications of cybersecurity practices, including privacy, data protection, and compliance. Understanding legal frameworks and ethical considerations is crucial for mPower Tech's IT Consultation Service to guide organizations in developing policies that align with legal requirements and ethical standards. By incorporating legal and ethical perspectives, mPower

Tech ensures that cybersecurity practices are compliant, protect user privacy, and adhere to ethical principles.

Assessing the Effectiveness of Our Innovation

Determining the effectiveness of mPower Tech IT consultation services requires a comprehensive evaluation process that assesses the impact of their interventions on cybersecurity resilience. Here is an overview of key steps and sources that can be used to evaluate the effectiveness of the innovation:

Define Evaluation Objectives: Clearly articulate the specific objectives and outcomes that you want to measure. This could include factors such as improved employee awareness, reduction in security incidents, or enhanced response capabilities.

Select Evaluation Methods: Choose appropriate evaluation methods based on the objectives defined. Some common methods include surveys, interviews, observation, and analysis of security incident data. These methods can help gather quantitative and qualitative data to assess the effectiveness of mPower Tech's interventions.

Measure Awareness and Knowledge: Assess the level of cybersecurity awareness and knowledge among employees before and after implementing mPower Tech's training programs. Use surveys or knowledge assessments to gauge improvements in understanding and adherence to security practices. Comparing pre- and post-training results can help determine the effectiveness of the awareness programs.

Analyze Security Incident Data: Examine security incident data, such as the number and severity of incidents, before and after engaging mPower Tech's consultation services. A decrease in the frequency or impact of security incidents can indicate the effectiveness of the implemented interventions.

Conduct Employee Feedback: Gather feedback from employees who have participated in mPower Tech's training programs or have received their consultation services. Interviews or surveys can provide insights into the perceived effectiveness of the interventions and identify areas for improvement.

Benchmarking: Compare the organization's cybersecurity performance against industry standards, best practices, or similar organizations that have implemented mPower Tech's services. This external benchmarking can provide a broader perspective on the effectiveness of the innovation.

Long-term Monitoring: Continuously monitor the cybersecurity posture of the organization over time to assess the sustainability of the improvements achieved through mPower Tech's interventions. Regular evaluations can help identify any emerging challenges or the need for further enhancements.

Bringing Our Innovation to Life

Turning the innovation of mPower Tech IT consultation services into a reality requires careful planning, resource allocation, and execution. Here is a 2-page description of the key elements needed to bring this innovation to fruition:

Vision and Strategy: To transform mPower Tech IT consultation services into a reality, a clear vision and strategy are essential. This involves defining the overarching goals and objectives of the services, identifying the target market and customer segments, and determining the unique value proposition that sets mPower Tech apart from competitors. A well-defined strategy guides the entire development process and serves as a roadmap for success.

Team and Expertise: Building a competent and experienced team is critical for the success of mPower Tech IT consultation services. This includes professionals with expertise in

cybersecurity, IT consulting, training and awareness, project management, and business development. The team should possess a deep understanding of the human factor in cybersecurity and be capable of delivering comprehensive solutions to address this issue effectively.

Market Research: Conducting thorough market research is essential to identify the demand for mPower Tech's IT consultation services and understand the competitive landscape. This involves analyzing industry trends, studying customer needs and preferences, and evaluating potential market size and growth opportunities. Market research enables mPower Tech to tailor their services to meet the specific requirements of their target customers.

Partnerships and Alliances: Establishing strategic partnerships and alliances with other organizations in the cybersecurity ecosystem can enhance the capabilities and reach of mPower Tech. This includes collaborating with technology vendors, industry associations, academic institutions, and cybersecurity experts. Partnerships can provide access to additional resources, knowledge exchange, and opportunities for joint marketing and business development.

Service Development: Developing the mPower Tech IT consultation services requires a comprehensive approach. This involves designing a range of services that address different aspects of the human factor in cybersecurity, such as training programs, awareness campaigns, policy development, incident response planning, and technology solutions. Service development should be driven by industry best practices, emerging trends, and feedback from potential customers.

Implementation and Execution: Once the services are defined, the focus shifts to implementation and execution. This includes creating detailed project plans, allocating resources effectively, establishing appropriate governance and quality control mechanisms, and setting up

the necessary infrastructure and technology platforms. A well-executed implementation ensures the delivery of high-quality IT consultation services to clients.

Marketing and Sales: Promoting mPower Tech IT consultation services requires a comprehensive marketing and sales strategy. This involves developing a compelling brand identity, creating targeted marketing campaigns, leveraging digital channels, attending industry conferences and events, and building a network of satisfied clients who can provide referrals and testimonials. Effective marketing and sales efforts help generate awareness, attract customers, and drive business growth.

Continuous Improvement: To remain competitive and relevant in the ever-evolving field of cybersecurity, mPower Tech must emphasize continuous improvement. This includes actively seeking feedback from clients, monitoring market trends, incorporating emerging technologies and methodologies, and adapting the service offerings to address evolving customer needs. Regular assessment and refinement of the services ensure long-term success and client satisfaction.

Summary:

The next steps for mPower Tech involve implementing the insights gained from the project, leveraging lessons learned, and taking proactive measures to enhance the innovation. Throughout the journey, valuable knowledge has been acquired, along with important lessons that will shape future actions. Reflecting on the project, there are aspects that could have been approached differently for better outcomes.

Next Steps:

Implementation and Deployment: Execute the detailed implementation plan to bring mPower Tech IT consultation services to market. This includes setting up the necessary infrastructure, finalizing service offerings, and launching targeted marketing and sales campaigns.

Continuous Improvement: Emphasize a culture of continuous improvement by actively seeking feedback from clients, monitoring industry trends, and integrating emerging technologies and methodologies into the service offerings. Regularly evaluate and refine processes to ensure optimal performance and customer satisfaction.

Client Relationship Management: Foster strong relationships with clients by providing exceptional service, promptly addressing their concerns, and delivering on promises. Develop long-term partnerships that drive mutual success and generate positive word-of-mouth referrals.

Expansion and Growth: Explore opportunities for expansion into new markets or verticals. Continuously assess market demands and adapt services to meet evolving customer needs. Seek strategic alliances or acquisitions that can accelerate growth and enhance market presence.

Lessons Learned:

Customer-Centric Approach: Place a strong emphasis on understanding customer pain points, needs, and preferences. Incorporate their feedback throughout the development and implementation process to ensure the services align with their expectations.

Agile Development: Adopt an agile approach to service development, allowing for iterative improvements and flexibility in response to market demands. Regularly reassess the business strategy to ensure it remains aligned with industry trends and customer requirements.

Talent Acquisition and Retention: Invest in attracting and retaining top talent with expertise in cybersecurity, IT consulting, and related domains. Develop a supportive work environment that encourages innovation, collaboration, and professional growth.

Proactive Marketing and Networking: Implement a comprehensive marketing and networking strategy early on to raise awareness of mPower Tech and build a strong industry presence. Leverage digital marketing channels, participate in industry events, and establish strategic partnerships to expand the customer base.

Things to Do Differently:

Robust Market Research: Conduct more extensive market research to gain deeper insights into customer needs, competitive landscape, and market dynamics. This will provide a stronger foundation for decision-making and differentiation strategies.

Pilot Testing: Prioritize pilot testing of the IT consultation services with a diverse range of clients. This will allow for real-world validation, identification of potential challenges, and refinement of the services before full-scale implementation.

Risk Management: Implement a comprehensive risk management plan to identify and mitigate potential risks and challenges that may arise during the implementation and growth stages. Proactively address legal, regulatory, and security considerations to ensure compliance and trust.

Scalability Planning: Develop a scalability plan from the early stages to accommodate growth and manage increased demand effectively. This includes scalability of infrastructure, resources, and operational processes.

Reference:

1. Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. European Journal of Information Systems, 18(2), 106-125.

2. Sukumar, A., Mahdiraji, H. A., & Jafari-Sadeghi, V. (2023). Cyber risk assessment in small and medium-sized enterprises: A multilevel decision-making approach for small e-tailors.

3. Liao, Q. V., & Cheung, C. M. (2001). Internet-based e-banking and consumer attitudes: An empirical study. Information & Management, 39(4), 283-295.

4. Gerber, N., Gerber, A., & Volkamer, M. (2017). Exploring the impact of awareness measures on Phishing susceptibility. Computers & Security, 65, 135-150.

5. Gupta, M., & Hammond, M. (2013). Examining employees' information security awareness: A Literature review and directions for future research. Information Management & Computer Security, 21(3), 159-186.

6. Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of Internet security breach Announcements on market value: Capital market reactions for breached firms and Internet security developers. International Journal of Electronic Commerce, 9(1), 69-104.

7. Fagan, M. H., Lawrence, E. R., McKeown, M. G., & Woelk, D. J. (2006). Detecting insider Threats using linguistic analysis. IEEE Intelligent Systems, 21(4), 32-39.

8. Kirlappos, I., & Sasse, M. A. (2013). Security education against phishing: A modest proposal for a change in HCI curriculum. In Proceedings of the 2013 ACM SIGCHI Conference on Human Factors in Computing Systems (pp. 589-598).

9. Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97-102.

10. D'Arcy, J., Hovav, A., & Galletta, D. F. (2009). User awareness of security countermeasures and Its impact on information systems misuse: A deterrence approach. Information Systems Research, 20(1), 79-98.

11. Nissenbaum, H. (2004). Privacy as contextual integrity. Washington Law Review, 79(1), 101-139.

12. Lee, M. K., Kusbit, D., Metsky, E., & Dabbish, L. (2015). Working with machines: The impact of algorithmic and data-driven management on human workers. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (pp. 1603-1612).

13. Azmi, R., Tibben, W. & Win, T. K. (2018). Review of cybersecurity frameworks: context and shared concepts, Journal of Cyber Policy, 3:2, 258-283.

14. Bubukayr, M. A. S. & Almaiah, M. A. (2021). Cybersecurity Concerns in Smart-phones and applications: A survey. 2021 International Conference on Information Technology (ICIT), Amman, Jordan, pp. 725-731.

15. Daengsi, T., Wuttidittachotti, P., Pornpongtechavanich, P., and Utakrit, N. (2021). A Comparative Study of Cybersecurity Awareness on Phishing Among Employees from Different Departments in an Organization. 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), Cameron Highlands, Malaysia, pp. 102-106.

16. Rajeswary, C. & Thirumaran, M. (2023). A Comprehensive Survey of Automated Website Phishing Detection Techniques: A Perspective of Artificial Intelligence and Human Behaviors. 2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), Erode, India, pp. 420-427.

17. Falowo, O.I, S. Popoola, J. Riep, V. A. Adewopo, & J. Koch (2022). Threat Actors' Tenacity to Disrupt: Examination of Major Cybersecurity Incidents. IEEE Access, vol. 10, pp. 134038-134051.

18. Swar, B., & Hossain, L. (2020). Cybersecurity awareness and compliance in organizations: A systematic literature review. Computers & Security, 97, 102184.

19. Rothstein, H. G., & Burke, J. W. (2018). Evaluating Cybersecurity Training Programs: Evidence-Based Approach. Proceedings of the 51st Hawaii International Conference on System Sciences. doi:10.24251/hicss.2018.301

20. Serrano, A., & Ortega, J. (2020). Evaluating the effectiveness of cybersecurity training programs. Information & Computer Security, 28(1), 68-86. doi:10.1108/ICS-10-2018-0117

21. National Institute of Standards and Technology (NIST). (2018). Framework for Improving Critical Infrastructure Cybersecurity. Retrieved from https://www.nist.gov/cyberframework

22. International Organization for Standardization (ISO). (2017). ISO/IEC 27004:2016 Information technology — Security techniques — Information security management — Monitoring, measurement, analysis, and evaluation.

23. Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. Information & Management, 49(3-4), 190-198.

24. Dunlop, M., & Brewster, S. (2010). Mobile technology and security: An investigation into the perceptions and practices of IT professionals. International Journal of Mobile Human Computer Interaction (IJMHCI), 2(2), 31-44.

25. Zafar, A., Shah, M. A., Shah, S. H., & Ahmad, T. (2019). Cybersecurity awareness and security behavior of users: A systematic literature review. Journal of Computer and Communications, 7(12), 41-57.

26. an Niekerk, J. (2014). A governance framework for cybersecurity: A discussion of legal, ethical, and cultural aspects. In Proceedings of the Information Systems Education Conference (ISECON) (Vol. 31, No. 2957).