Strengthen of Cybersecurity in the Organizations: Challenges and Solutions

Abdulaziz Alarifi
Computer Science Department, Community College, King Saud University
Riyadh 11437, Saudi Arabia

ABSTRACT
The adoption of technological resources in organizational functions reflects the changes in the nature of interactions in society. Business communication involves interactions meant to realize organizational functions such as supply, marketing, logistics, and sales, among others non-business functions. The utilization of technological resources in organizations is inevitable in the current environment. This is made possible by the advancement in technologies such as the Internet and communication devices. The paper examines the challenges and solutions related to cybersecurity. The vice has been prevalent in recent times; with companies making huge losses on finances and data. The proposed holistic solutions will require close cooperation between public, organizations, and government to stimulate the chances of success.

Keywords
Cybersecurity, data threats, Information Security, organizations data protection, Internet security solutions.

1. INTRODUCTION
Since the invention of the Internet in 1994, the corporate world has changed significantly. It is noteworthy that the virtual environment created through the Internet has been adopted across communities to ease interactions. Technology allows users to easily communicate, share ideas, and relay information that is relevant to business functions. Therefore, companies have a duty to facilitate the use of active online systems to enhance the realization of the set objectives.

The development of electronic computing and communication technology in the recent past has contributed to increased threats propagated through computer systems – both online and offline. The new class of threats has great potential to jeopardize the capacity of society in promoting internal and external order at local as well as international levels. It is noteworthy that nations are different stages in the networked society although the nature of threats and perpetrators is sometimes hard to reveal. Government players, especially within the security circles, have also been accused of using computer technology to realize socio-political goals. The social media networks have provided a variety of platforms for perpetrators to engage in information warfare and deception in a manner that brings disharmony in society. Therefore, there is a great need for society to appreciate that cyber-threats require utilization of stiffer and stringent mitigation mechanism backed by uniform laws at the international level.

2. STATEMENT OF THE PROBLEM
The world continues to experience different forms of planned crimes that change with time and formation due to technological advancement. The preparation aspect of the concept emerges from the fact that the culprits appear trained and systematized. Over the last few decades, global dynamics have changed owing to technological advancement, socio-political alignments, and international security. As such, potential criminals take advantage of the changes to adopt new formations of organized crime [1]. Yar [2] recognize that the world is now more interconnected, with societies facing increasing threats. Criminal organizations and individuals take advantage of the situation to extort money from people as well as engage in unlawful activities such as cybercrimes [3]. It is also noteworthy that culprits have moved from the traditional entities of crimes such as robbery with violence to the virtual world in line with technological advancement.

Moreover, fraud and financial crimes through virtual platforms have been on the increase thus hurting the economy and business operators [4] [5]. In a research study by McAfee, the firm estimated that the global economy is losing over 445 billion dollars due to cybercrimes every year. In Hong Kong, authorities reported that the country lost HK$2.3 billion in 2016 alone. The figure could be higher due to unreported cases throughout the region. Ina recent incident of cybercrime in the city, hackers locked personal data of WWPKG Holdings' customers claiming to be given bitcoin ransom. The technology crime team helped in unlocking data; hence, safeguarding the privacy of the clients. Cases of cheating and deception have increased as perpetrators utilize email and phone frauds to lure naïve citizens.

Authorities and organizations have come with several measures to monitor and deter cybercrimes, although the interventions have not been enough since culprits are all over the world. There have been attempts to make the commercial crime bureau effective to prevent organizations from making business losses [6]. Unfortunately, tech-savvy individuals can hack devices and online sites without the knowledge of the victims. Prevention is essential to reduce the vulnerability of the city to online criminals in the modern world [7]. Since the late 2000s, police officers have made cyber crime a priority area that should be tackled appropriately. It is recognized that the formulation of preventive measures is a significant challenge that authorities, organizations, and individual citizens need to work on for their benefit.

Robert James from ITProPortal [8] has stated that the threat of the data breach has affect even the big companies. For example, Facebook admitted that around 50 million users were compromised by the security breach. Furthermore, Uber has paid £133m to settle the legal penalization owing to the cyber-attack which happened to expose 57 million customers and driver data. British Airways also had to face the cybersecurity breach which affected around 380,000 transactions. This catered the stolen personal and financial data. As a result, the average cost of the data breach to the companies worldwide will be millions of U.S. dollars [8]. The previous examples clearly shown the need for cybersecurity strong practices are very important to avoid or reduce the risks.

3. METHODOLOGY

Qualitative method has been used as a strong background about the topic. The literature review has been involved to show the related topics. This paper has used a systematic review which is a scientific approach that can be used to review data systematically by identifying and summarizing the related evidences.

4. DISCUSSION OF CURRENT ISSUES AND CHALLENGES

Computer crime is recognized as an organized attack on computer programs, data, and systems for purposes of bullying or threatening the targets. This form of threat necessitates the use of the computer as a perpetrator or target. It normally involves intrusion to an information system of another party for purposes of causing disruptions or mining data [9]. An attack on critical infrastructure is not only destructive to a country's economy but also harmful to the lives of the citizens. Critical infrastructure includes defense system, nuclear sector, financial services, and information technology industry, among others [10]. Imagine an attack on the nation's power grid using a program that can switch off or undermine the billing system. Such an attack would have irreparable and disastrous consequences on the country's economy [11] [12]. Most areas in the manufacturing sector would stop operating; causing loss of billions of dollars within a short period. Other sectors such financial industry would also suffer in a similar due to the high utilization of energy to power machines. The financial sector has also been targeted in several cyber terror acts [13]. The industry has great importance in the social and economic well-being. An attack would lead to the loss of crucial data and money [14]. Another disastrous attack would be on the defense system. Such an attack would expose the technologies utilized by the department of defense; thus, undermine national security to a large extent. The government needs to closely monitor all suspicious activities regarding cyber-security by working closely with the specific players in researching for better mitigation measures.

Computer hacking is the unauthorized access to computer systems of another party with the aim of stealing, changing or destroying information. This involves the installation of malware without the consent of the authority [15]. Manipulation of electoral data has adverse effects on undermining the tenets of democracy. This may not carry similar impacts as other sectors but there is a great need to ensure proper measures are put in place to safeguard the country's political leadership. It is necessary to understand the terminologies used in digital terrorism to avoid misleading the public as well as assist in creating proper prevention strategies.

Information warfare is recognized as manipulation of data and computer technologies to achieve an advantage of others. This may involve denial of information or presentation with incorrect data that end up undermining one's objectives. Information warfare may involve electronic warfare, information attacks, and psychological operations, among others [16]. From the Russian perspective, it involves attacking or blocking systems that are being used by an opponent. This entails activation or denial of vital information. The Chinese consider information warfare as it as an opportunity to help in making advancements in their military to realize success in the battlefield. North Korea sees information warfare as an opportunity to mislead the developed nations in their efforts to develop nuclear weapons. The country believes in blocking access to vital data by opponents as well as information sharing to hide their activities from attack in a similar manner as Iran in 2010. The American perspective is that information warfare presents an opportunity for defense agents to work on better programs and approaches to improve military technologies [17]. The process may involve denial of information or activation in production and transmission of data. Nations around the world are using information warfare to gain an advantage in readiness for military preparedness through advanced technologies.

Bullock, Clarke, & Tilley [18] observe that criminal networks act as places of socialization where the culprits engage in organized and properly-connected illegal activities. Such groupings have been in existence for a long time although the structural formations and objectives change with time. The dynamics in the modern world have contributed to changes in the organization of organized criminal gangs [18]. Technological advancement, globalization, and terrorism are some of the contemporary issues that affect the organization of organized criminal gangs. Organized gangs are extremely powerful and influential in society. Often, they compromise the socio-political and economic leaders for protection through policies and legislation. In the coming days, the operations of organized criminal gangs are likely to change to create a safe haven for their activities [19]. One likely scenario is the internationalization of operations through expansion and collaboration [20].

Advancement in technology has brought new challenges and threats to the world economy. Apparently, as observed by Tcherni, Davies, Lopes, & Lizotte [21], the uptake of e-commerce has seen thefts of credit data through hacking. Many people are unaware of the appropriate methods to protect their data from loss and hackers. In a survey conducted by Javelin Strategy and Research, the group observed that over Americans lost over 20 billion dollars due to identity theft in 2013 alone [22]. Organized crimes gangs around the world operate in a similar manner although appear sophisticated and powerful. For instance, immigrants from China and Russia enter the US where they engage in illegal commercial activities and gambling. Another concern is globalization that has created room for terrorism [23].

Social media attracts several drawbacks that should always be avoided within an organization. The OSN platforms attract security issues and loss of data that jeopardize private information about a company or respective stakeholders [24]. For instance, a company employee may send private company information to unintended audiences. Such information ruins the business image. Some companies have attracted the wrath of the public due to leaked emails [25]. It is also noteworthy that online crimes through hacking undermine the capacity to control the flow of information. For instance, Yahoo Inc. has been a victim of occasion hacking which results in manipulation of customers' information. Many other firms have fallen into victims of miscommunication due to social media engagement. Therefore, it is prudent for a company to have a clear online engagement plan to reduce adverse effects on business communication.

In the current information age, data is susceptible to loss and manipulation arising from computer crimes. Hautala [26] observes that data privacy is an important issue that generates numerous social, political and integrity issues. There exist concerns about the disclosure of individual and/or organizational information. It is expected that data available should be guarded to enhance the interests of owners. Hautala [26] is concerned no one is safe owing to the complicated

nature and dynamics of technology. The article highlights that combating cybercrime will require the users to identify appropriate approaches that will safeguard their data as well reduce the exposure of their systems. Just recently, Kaspersky Lab observed that nobody is safe in the wake of increased cases of cybercrime. The company's systems were recently hacked hence putting their information vulnerable [26].

In examining computer crime and legal frameworks around the world, Easttom & Taylor [27] observe that nations are yet to come with uniform cybercrime laws. Interestingly, government websites and computers are regularly hacked around the world, including the US government that has highly advanced in technology. The authors underscore the significance of elaborate control on the movement of data either electronically or physically reduce the risk exposure. Data protection requires the integration of various approaches covering the users, processes, and systems. The implication of the study is to inform the regulators on areas that require greater relook. Securing the network is essential using policy, audit, and effective controls. Easttom & Taylor [27] assert that multiple approaches through encryption, integrity protection, and data loss prevention techniques are essential in enhancing the data is adequately protected. The findings reveal the importance of safeguarding the integrity of the data to ensure it is not compromised either by external or internal users.

5. SOLUTIONS

A liability regime would compel the content carriers to ensure distribution of the right information to the public. The carriers have the capacity to create systems that will help in the approval of content before it is relayed or released to the public [28]. Nonetheless, such a move would undermine the commercial interests of the service providers by making the business unsustainable. With the high number of users and sites, service providers are likely to encounter challenges in enforcing and implementing the proposed regulations in different regions. Companies such as Yahoo and Google cannot effectively monitor the billions of users due to the possibility of creating burdens on users and intermediaries [28]. The move has the potential to increase costs for basic services that are normally free, hence, undermine efforts to improve connectivity in the world. There is a proposed total immunity model that seeks to protect providers from any nature of information or content disseminated through their platforms. In doing so, the ISPs will be required to remove contents that appear undesirable [29]. They will also be required to address the interests and always needs of the users.

The current regulations strive to restrict the liability of the internet service providers (ISPs). It is considered that an elaborate framework to guide the e-commerce sector should consider the divergent interests of stakeholders [30]. Nonetheless, the proposed plans have the potential to lead to adverse effects. It is notable that the industry faces significant challenges due to dissimilar treatments by the member states. In the same vein, countries lack uniform laws to help in protecting the rights and interests of the service providers and stakeholders. The society needs to recognize the significance of the ISPs in the global economy, especially the dissemination of information. Proper and effective rules and policies should aim at safeguarding the interests of both the users and service providers.

Also, companies should safeguard data using effective strong legal procedures and regular IT security audit. The considerations on the internet should include but not limited to usage, security, environmental impacts, privacy, and control [31]. The authorities need to work towards safeguarding the interests of the consumers, trade on the Internet, and assessment while strengthening policies in readiness for the emerging challenges. Precedent in a court procedure regarding internet cases helps in setting the ground for improved legislation and consumer protection as well as creating standards that guide the business. These may affect the ruling in a case; thus, should be used in rather an intelligent approach [31].

Organizations need to create agencies alongside the cybersecurity and technology crime bureaus in police departments should be created to handle cyber-crime related issues. The bodies will be responsible for performing crime investigations, prevention, and forensic examinations. Companies with such arrangements claim that the agency is helpful in investigating cyber-crimes while at the same time creating awareness on mitigation measures. The government should ensure companies and the public takes the rightful duty in curding computer crimes [32]. It has also emerged that the law enforcers need to work in close collaboration with the banking sector to stop funds transfer once detected. The banks not only stop the transfer but also freeze the accounts. The move should be backed stringent of legislation on cybersecurity to grant the legal framework to net criminals.

Private companies have a role to play in the protection of users and clients from being victimized through online criminality. Unfortunately, there exist some barriers to establishing data commons for economic development such as security, data personalization, privacy, and human capital. The barriers limit access to information or at times jeopardize the private data about the users [33]. To become a data-driven organization, a firm needs to establish its metrics that enhance success. It is also important to have the right technology resources and human capital to transit effectively. Another important consideration is undertaking a clear and detailed business intelligence to identify approaches to gather and utilize data for the benefit of the company. Big social data is subject to 'lens distortion' in that users can utilize the available applications to manipulate information. The trend has seen the creation of incorrect information that lacks facts and credibility. Distortion can be reduced through censorship of information by the service providers. Enhancing the rules of communication and awareness can also assist in eliminating incidences of distortion. The government regulators should also advice private companies to limit data before moving their data to the cloud [34]. Such an understanding enables an organization to take the best approach in the application keys' security and encryption controls.

Equally, the strategy toward creating an appropriate online engagement is pegged on the needs and interests of an organization. Business communication should be improved by taking the right step in making the right choice of platforms. The social networks should be less susceptible to hacking and data loss. Furthermore, there is a need to enhance the quality of message contents to reduce the chances of a ruined image in case of information leakage. The messages and videos posted on social media platforms should reflect the intentions and interests of a company [35] [36]. Nevertheless, it is prudent to consider the interests of target groups for ease of acceptance. The digital team in an organization has a responsibility to work closely with other teams to ensure the development of the right message content.

6. CONCLUSION

Computer crime has taken shape over the last two decades due to considerable advancements and research on better computing and communication technologies. Threats emerging from digital terrorism have the potential to lead to another global as nations are utilizing the opportunity to engage in actions that threaten national and global security. Companies, especially the most vulnerable should have effective control and mitigation measures. Also, it is rightly important for the development of stringent legislation and uniform policy framework regarding digital terrorism. It is also notable that computer crime can take place from a remote location as long as one has access to computer systems, programs, and data. The attacks undermine the economy but also threaten national and international security. This is the reason the country has engaged in various acts of information warfare to achieve their dominance and leadership in military technology. It is prudent for the international community to address the growing concerns and challenges arising from cyber-terrorism in the contemporary world.

7. ACKNOWLEDGMENTS

This research was supported by King Saud University, Deanship of Scientific Research, Community College Research Unit.

8. REFERENCES

[1] Mccarthy, D. M. P. 2013. Economic history of organized crime: A national and transnational approach. Place of publication not identified: Routledge.

[2] Yar, M. 2013. Cybercrime and society. Sage.

[3] Kshetri, N. 2013. Cybercrime and cybersecurity in the global south. Springer.

[4] Asghari, H., van Eeten, M., and Bauer, J. M. 2016. 13. Economics of cybersecurity. Handbook on the Economics of the Internet, 262.

[5] Kesharwani, A. and Tripathy, T. 2012. Dimensionality of perceived risk and its impact on Internet banking adoption: An empirical investigation. Services Marketing Quarterly, 33(2), pp.177-193.

[6] Broadhurst, R. and Chang, L.Y. 2013. Cybercrime in Asia: trends and challenges. In Handbook of Asian criminology (pp. 49-63). Springer, New York, NY.

[7] Min, K. S., Chai, S. W., and Han, M. 2015. An international comparative study on cyber security strategy. International Journal of Security and Its Applications, 9(2), 13-20.

[8] Robert J. 2018. Biggest cyber security breaches. ITProPortal.https://www.itproportal.com/features/biggest-cyber-security-breaches-2018/

[9] Cavelty, M. D., and Mauer, V. 2016. Power and security in the information age: Investigating the role of the state in cyberspace. Routledge.

[10] Ashibani, Y., and Mahmoud, Q. H. 2017. Cyber physical systems security: Analysis, challenges and solutions. Computers & Security, 68, 81-97.

[11] Robinson, M., Jones, K., and Janicke, H. 2015. Cyber warfare: Issues and challenges. Computers & security, 49, 70-94.

[12] Wells, L. J., Camelio, J. A., Williams, C. B., and White, J. 2014. Cyber-physical security challenges in manufacturing systems. Manufacturing Letters, 2(2), 74-77.

[13] Lagazio, M., Sherif, N., and Cushman, M. 2014. A multi-level approach to understanding the impact of cyber crime on the financial sector. Computers & Security, 45, 58-74.

[14] Dawson, M., Omar, M., and Abramson, J. 2015. Understanding the methods behind cyber terrorism. In Encyclopedia of Information Science and Technology, Third Edition (pp. 1539-1549). IGI Global.

[15] Mann, I. 2017. Hacking the human: social engineering techniques and security countermeasures. Routledge.

[16] Levi, M. 2017. Assessing the trends, scale and nature of economic cybercrimes: overview and issues. Crime, Law and Social Change, 67(1), 3-20.

[17] Hutchinson, W. 2006. Information warfare and deception. Informing Science, 9.

[18] Bullock, K., Clarke, R. V. G., and Tilley, N. 2010. Situational prevention of organised crimes. New York, NY: Taylor & Francis.

[19] Sadeghi, A. R., Wachsmann, C., and Waidner, M. 2015, (June). Security and privacy challenges in industrial internet of things. In Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE (pp. 1-6). IEEE.

[20] Taylor, R. W., Fritsch, E. J., and Liederbach, J. 2014. Digital crime and digital terrorism. New Jersey, NJ: Prentice Hall Press.

[21] Tcherni, M., Davies, A., Lopes, G., and Lizotte, A. 2016. The dark figure of online property crime: Is cyberspace hiding a crime wave?. Justice Quarterly, 33(5), 890-911.

[22] Roberts, L. D., Indermaur, D., and Spiranovic, C. 2013. Fear of cyber-identity theft and related fraudulent activity. Psychiatry, Psychology and Law, 20(3), 315-328.

[23] Abadinsky, H. 2012. Organized crime. Boston, MA: Cengage Learning.

[24] Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., and Qiu, D. 2014. Security of the Internet of Things: perspectives and challenges. Wireless Networks, 20(8), 2481-2501.

[25] Wang, T., Zheng, Z., Rehmani, M. H., Yao, S., and Huo, Z. 2018. Privacy Preservation in Big Data from the Communication Perspective—A Survey. IEEE Communications Surveys & Tutorials.

[26] Hautala, L. 2015. None of us are safe: Major cybersecurity company hacked. Retrieved December 11, 2018, from CBS Interactive Inc.: http://www.cnet.com/news/none-of-us-are-safe-major-cybersecurity-company-hacked/

[27] Easttom, C., and Taylor, J. 2010. Computer crime, investigation, and the law. Boston, MA: Course Technology, a part of Cengage Learning.

[28] Palazzi, P., and Marco, R. J. 2015. "Search Engine Liability for Third Party Infringement: A Keenly Awaited Ruling." Journal of Intellectual Property Law & Practice, (10)(4): 244-245.

[29] Jakobsen, S. S. 2011. "Mobile Commerce and ISP Liability in the EU." International Journal of Law and Information Technology, 29-52.

[30] Edwards, L. ed. 2005. The new legal framework for e-commerce in Europe. Bloomsbury Publishing.

[31] Menestrel, M. L., Hunter, M., and Bettignies, H.-C. d. 2002. Internet e-ethics in confrontation with an activists' agenda: Yahoo! on trial. Journal of Business Ethics , 135-144.

[32] Holt, T.J. and Bossler, A.M. 2015. Cybercrime in progress: Theory and prevention of technology-enabled offenses. Routledge.

[33] Sood, A.K., Bansal, R. and Enbody, R.J. 2013. Cybercrime: Dissecting the state of underground enterprise. Ieee internet computing, 17(1), 60-68.

[34] Do, Q., Martini, B., & Choo, K. K. R. 2015. Exfiltrating data from Android devices. Computers & Security, 48, 74-91.

[35] Wells, A. 2013. The importance of design thinking for technological literacy: A phenomenological perspective. International Journal of Technology and Design Education, 23(3), 623-636.

[36] Wong, K., Wong, A., Yeung, A., Fan, W., and Tang, S. K. 2014. Trust and privacy exploitation in online social networks. IT Professional, 16(5), 28-33.