Communications sector infrastructure

Communication exchange system has become a crucial component in our lives today. Many businesses have thrived in connection with a viable communication system. This is a way in which a marketer has seen his firm optimize and maximize profits as a real interaction between him, and the consumer is enabled by the availability of communication system. Apart from that communication sector prevails in areas such as security department, finance department, transport department and many other critical sectors (Lewis, 2014). The finance department requires communication infrastructure in conjunction with other junior departments in harmonizing financial records as well as monetary gains from the business. Transportation department currently is being controlled using communication infrastructure in setting arrival and departure time for various journeys (DHS, 2015).

Communication connections are mostly run by the private sector in the presence of Continuity Guidance Circular (CGC) which offers directions to the Non-Federal Governments (NFGs) on how to ensure the effectiveness of the program (FEMA, 2013). This circular encompasses all forms of organizations from tribal, local government, territorial and other non-governmental forms. All forms of communication are integrated into one unit and fed into the system using the internet (FEMA, 2013). This communication platform has evolved in proportional to cyber-attack. This is a threat lagging private sector behind in dissemination of quality services to its members. It is no doubt that many firms do not consider to carry out research on how well to protect their communication systems in case of an attack. All that they concentrate on is the profits to be collected (Etzioni, 2011). This is one of the many weaknesses many firms face and the issue needs to be addressed. Still, the

transitions in the communication technology platform have positively yielded success on the part of hackers who are in the frontline of innovations progress (DHS, 2015).

Due to increased cases of hacking, the private sectors are left with no idea in which to discharge their responsibilities properly. Interconnection of computers to perform a central task has proved unworthy irrespective of many experts put in place to control the system (Ra'ed & Keating, 2014). This implies that consumers do not get their ordered products on time or else they lack information concerning a new product which might have been introduced in the market by their respective firms. This form of cyber-attack may come in as a result of competition for market domination by various antagonistic investors (Etzioni, 2011).

Program Goals

United States retains two guiding programs Continuity of Government (COG) and Continuity of Operations (COOP) which lay a foundation upon which every goal and vision of a given organizations are determined (DHS, 2015). This also ensures that citizens are offered only those services essential to them. In this case, all objectives, goals, and visions of the firm need to be reviewed. The private sector cannot solve the problem of cyber theft if the entire member companies do not comprehend the driving force to their business venture (Stergiopoulos et al., 2017). In 2008, George W. Bush signed Comprehensive National Cyber Security Initiative (CNCI) to secure communication attack for current and future economy. He urged all the stakeholders to focus on one goal, and that is cyber threats reduction

(Hennig & Rollins, 2009). Also, the agreement was cemented on the grounds of how the member firms and federal governments shared benefits. All goals of a business are met by satisfying the consumer needs. This assessment is important to the stakeholders in sending the right information to the government for the arrangement of support provision. It also indicates how many objectives the firm has been able to achieve during the operation period (Hennig & Rollins, 2009).

Discharge of Duties and Monitoring of Staff

National Institute of Standard and Technology (NIST) department to set peculiar critical standards upon which communication infrastructure would be conducted (DHS, 2015). The key issue is how leadership is done and closes monitoring of the staff. Today’s private sector should incorporate all the necessary information concerning the best infrastructure platform which would otherwise cope with cyber-attack menace (Knapp & Langill, 2014). This is possible through the in-depth search of information the hackers might be using in lagging the economy behind. Once this information is collected, a firm background in collaboration with the government should be laid. This could only be achieved by enhancing a new database with new security coding system that could easily be manned from a central point (Knapp & Langill, 2014).

The databases should be enabled with data tracking mechanisms to detect all the specifications and the identity of any intruder into the system (Kotzanikolaou et al., 2013). The operating staff and their information should be easily monitored; should there be information leakage, tracing of the

culprit will be easy. The government in line with the private sector should impose harsh rules that will apply to anyone who tries the cyber attack on all grounds (DHS, 2015). Again the consumers should be included in decision-making to ensure that the implementation of new communication system doesn’t throw them out of business on the grounds of its operation and the guidelines.

Communication Technology Assessment

In every aspect of business operation, the introduction of a new mechanism of services is bound to yield setbacks which in this case are referred as risks. One of the greatest risks a private sector should be aware of is the ability to lose some of the stakeholders (Yan et al., 2013). This comes with new principles that would guide the operations of the system in securing a given department. For instance, change in the systems in the security department may imply that some of the operators have to be axed since the new system is capable of operating various sections that were earlier performed by different personnel. This is a significant threat since the fired individuals might be containing critical information that would interfere with the safety of department in case they decide to retaliate.

Risk Evaluation

The magnitude of a threat to the new system should be evaluated. In the security department, for instance, the axing of various departments and their operation staff should be closely reviewed. Because these experts still contain many secrets of the entire security staff, the option to send them home is utterly inappropriate. This is supported by the argument that in

situations of retaliation by this group. In the government sector, a threat may impact severe consequences due to its broadness in management level and corruption scenario which remains to be a significant threat to success. Risk assessment can still be determined by the loss a firm will incur regarding devotion and money.

Risk Management

This is another area that requires attention in determining how the cyber-attacks can be managed. Application of approaches that lead to quality progress and effectiveness of the program should be the guiding principle of the government (FEMA, 2013). Registering, scanning and monitoring every step the operating team undertakes is another important measure to mitigate cyber theft. Still, on that ground, security department should strictly observe the person entitled to run the system (May & Koski, 2013

The mission to improve the communication system targeting their counterparts will probably be aborted mainly through leaking of information. The system should be designed in a manner that it won’t access any codes from outside the base. Just in case the hackers succeed in collapsing the system, the whole system should be set in a manner which destroys everything. This will assist in controlling cyber attacks in many fields of operation.

Assessment of Program’s Readiness

The success of the whole operation should be measured by looking at how the business is running. In the case of improved profit margins and customer

satisfaction, the operation of the system should prove applicable. This is contributed by strong leadership originating from senior positions at the junior level (Younis & Kifayat, 2013). On the other hand, if the system runs in a reverse manner, it implies that the cases of cyber threat were not controlled. The firm and the government should work on adding more knowledge and pooling resources together to curb losses which would deteriorate the economy.

It is crucial for business and security firms to move with technological advancements that are changing on a daily basis. It is a wise decision to do away with out of date technologies that are prone to cyber-attacks and embrace those which are secured against such threats. Communication infrastructure forms an integral part of any company and has a direct impact on performance. As such, maintaining the integrity of the infrastructure is critical. The Continuity Guidance Circular (CGC) offers directions to Non-Federal Governments (NFGs) on how to ensure the effectiveness of the program. The CGC provides a guideline on the dissemination of duties, continuous assessment of the infrastructure, risk management, and evaluation and also the assessment of the program’s readiness (FEMA, 2013).

References

Department of Homeland Security, (2015). Communications Sector-Specific Plan an Annex to the NIPP 2013. Retrieved from https://www. dhs. gov/sites/default/files/publications/nipp-ssp-communications-2015-508. pdf

Etzioni, A., (2011). Cybersecurity in the Private Sector. *Issues in Science and Technology.* Retrieved from http://issues. org/28-1/etzioni-2/

Federal Emergency Management Agency, (2013). Continuity Guidance Circular 1 (CGC 1) Continuity Guidance for Non-Federal Governments (States, Territories, Tribes, and Local Government Jurisdictions). Retrieved from https://www. fema. gov/media-library-data/1386609058803-b084a7230663249ab1d6da4b6472e691/CGC-1-Signed-July-2013. pdf

Hennig, A & Rollins, J., (2009). Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations. *Congressional Research Service.* Retrieved from https://fas. org/sgp/crs/natsec/R40427. pdf

Knapp, E. D., & Langill, J. T. (2014). *Industrial Network Security: Securing Critical Infrastructure networks for the smart grid, SCADA, and other Industrial Control Systems* . Syngress. Retrieved from http://library. books24x7. com. ezproxy2. apus. edu/toc. aspx? bookid= 77754

Kotzanikolaou, P., Theoharidou, M., & Gritzalis, D. (2013). Assessing n-order dependencies between critical infrastructures. *International Journal of Critical Infrastructures 6* , *9* (1-2), 93-110

Lewis, T. G. (2014). Critical Infrastructure Protection in Homeland Security. Somerset: John Wiley & Sons, Incorporated. Retrieved from http://ebookcentral. proquest. com. ezproxy2. apus. edu/lib/apus/detail. action? docID= 1813343

May, P. J., & Koski, C. (2013). Addressing public risks: Extreme events and critical infrastructures. *Review of Policy Research* , *30* (2), 139-159.

Retrieved from http://onlinelibrary. wiley. com. ezproxy2. apus. edu/doi/10. 1111/ropr. 12012/full

Ra'ed, M. J., & Keating, C. B. (2014). The fragility of oil as a critical infrastructure problem. *International Journal of Critical Infrastructure Protection* , *7* (2), 86-99. Retrieved from https://pdfs. semanticscholar. org/745d/aa0b70a3e6ced165add2435036ab903bc999. pdf

Stergiopoulos, G., Kotzanikolaou, P., Theocharidou, M., & Gritzalis, D. (2017). Risk Mitigation for Critical Infrastructures: AUEB INFOSEC Lab Initiatives. Retrieved from https://infosec. aueb. gr/Publications/Risk-Tea%202017A %20CIP. pdf

Yan, Y., Qian, Y., Sharif, H., & Tipper, D. (2013). A survey on smart grid communication infrastructures: Motivations, requirements, and challenges. IEEE Communications Surveys & Tutorials, 15(1), 5-20. doi: 10. 1109/SURV. 2012. 021312. 00034

Younis, M. Y. A., & Kifayat, K. (2013). Secure cloud computing for critical infrastructure: A survey. Liverpool John Moores University, United Kingdom, Tech. Rep. Retrieved from https://www. researchgate. net/profile/Younis_A_Younis/publication/262817790_Secure_Cloud_Computin g_for_Critical_Infrastructure_A_Survey/links/5465ed3e0cf2f5eb180130d5. pdf