**18021370**

To justify my research I have got vast amount of information through various resources. I’ve found the required information through google scholar, ACM digital library and science direct by searching with certain keywords that are related to my research question.

My research question which I had submitted is,

**Research Question:** Why do cybersecurity teams are opting by less number of organizations in this modern technology driven world where cyberattacks, data theft are happening frequently?

1. **The population:** Software engineers.
2. **The intervention:** Software development team, administration of organizations.
3. **The comparison:** Penetration testers vs. cybercriminals.
4. **The outcomes:** Motivates the organizations by explaining current threats and upcoming growth in cybercrimes which leads to the increase of cybersecurity teams in organizations.
5. **The context:** Rescuing the organizations from cyberattacks (Involving previous records as well as the survey records to represent the complexity in this aspect).

The keywords which I used to search for the information are:

1. Cyber teams
2. Cyber attacks
3. Penetration testers
4. Current cyber threats in organizations
5. Threat management

Here are the references list which I got by searching with the above keywords which are related to my research question and helped me in obtaining information to my research.

***Cyber Teams:***

1. Finkle, J., Hosenball, M. (2014). Exclusive: More U.S. retailers victims of cyber attacks – sources. Reuters, Sun January 12th.

2. Futoransky, A., Miranda, F., Orlicki, J., Sarraute, C. (2009). Simulating cyber attacks for fun and profit. Proceedings of the 2nd International Conference on Simulation Tools and Techniques.

3. Klein, G., Calderwood, R., Clinton-Cirocco, A. (2010). Rapid decision making on the fire ground: The original study plus a postscript. Journal of Cognitive Engineering and Decision Making, 4(3), 186-209.

***Cyberattacks:***

4. Eric Byres and Dan Hoffman, Nate Kube On Shaky Ground — A Study of Security Vulnerabilities in Control Protocols, [online] Available: <http://byressecurity.comlassets/pdf/On%20Shaky%20Ground%20-%20NPIC_HMIT_2006%20Paper.pdf>.

5. Daniel Lough, A Taxonomy of Computer Attacks with Applications to Wireless Networks, 2001.

6. Bonnie Zhu and Shankar Sastry, "SCADA-specific Intrusion Detection/Prevention Systems: A Survey and Taxonomy", proceedings the First Workshop on Secure Control Systems (SCS’10), 2010.

7. S. Kamara, S. Fahmy, E. Schultz, F. Kerschbaum, and M. Frantzen. Analysis of vulnerabilities in Internet firewalls. *Computers & Security*, 22(3):214--232, Apr. 2003.

***Penetration Testers***:

8. W. Dawoud, I. Takouna, and C. Meinel. Infrastructure as a service security: Challenges and solutions. In *Proc. 7th International Conference on Informatics and Systems (INFOS)*, Mar. 2010.

9. T. Wood, E. Cecchet, K. K. Ramakrishnan, P. Shenoy, J. van der Merwe, and A. Venkataramani. Disaster recovery as a cloud service: Economic benefits & deployment challenges. In *Proc. HotCloud*, June 2010.

10. D. Merkel. Docker: Lightweight Linux containers for consistent development and deployment. *Linux J.*, Mar. 2014.

11. C. Clark, K. Fraser, S. Hand, J. G. Hansen, E. Jul, C. Limpach, I. Pratt, and A. Warfield. Live migration of virtual machines. In *Proc. NSDI*, pages 273--286, May 2005.

***Current cyber threats in organizations***:

12. Marlborough M. Raytheon to develop cyber maneuver technology for US Army: Proactive cyber approach to improve network defense in high-threat environments [Internet]. Waltham: Raytheon Company; c2015 [updated 2012 Jul 16; cited 2017 Jul 26]. Available from: [http://raytheon.mediaroom.com/index.php?s=43&item=2136](http://raytheon.mediaroom.com/index.php?s=43%26item=2136).

13. Desk N. Cyber maneuvering and morphing—Are defense networks on course to “self awareness”? [Internet]. Qadima: Defense Update; c2002–2017 [updated 2012 Jul 21; cited 2017 Jul 26]. Available from: <http://defense-update.com/20120721_raytheon-to-develop-cyber-maneuver-technology-for-us-army.html>.

14. Beraud P, Cruz A, Hassell S, Meadows S. Using cyber maneuver to improve network resiliency. In: Proceedings of the 2011 Military Communications Conference; 2011 Nov 7–10; Baltimore, MD, USA. Piscataway: Institute of Electrical and Electronics Engineers; 2011. p. 1121–6.

***Threat Management:***

15. Fransen, F. et al. 2015. Cyber security information exchange to gain insight into the effects of cyber threats and incidents. e & i Elektrotechnik und Informationstechnik. 132, 2 (2015), 106--112.

16. Sommer, R. and Paxson, V. 2010. Outside the closed world: On using machine learning for network intrusion detection. Security and Privacy (SP), 2010 IEEE Symposium on (2010), 305--316.

17. Fransen, F. et al. 2015. Cyber security information exchange to gain insight into the effects of cyber threats and incidents. e & i Elektrotechnik und Informationstechnik. 132, 2 (2015), 106--112.