A STUDY ON THE IMPORTANCE OF CYBER SECURITY LAB IN AN UNDERGRADUATE CYBER SECURITY PROGRAM

Munther Abualkibash[1]

[1]*School of Information Security and Applied Computing, College of Technology, Eastern Michigan University, USA*

Abstract

There is an urgent need to enhance cyber security education and research by creating a lab to promote active and project based learning in the field of cyber security. The lab should be utilized as a source to educate and train future generations of cyber security professionals and researchers to meet the demand of public and private organizations. The fast developments in cyber security along with increasing threats of hacking to private and public institutions require a comprehensive readiness plan. A critical component of this plan is to have a solid foundation of education infrastructure to prepare college graduates with the state-of-the-art knowledge to defend against any cyber threats.

Keywords: *Cyber security*

----------***----------

1.INTRODUCTION

There is a huge demand for highly qualified individuals with a deep understanding of cyber security defensive techniques. Therefore, each undergraduate cyber security program should plan to create a cyber security Lab to advance the students' knowledge with the fundamental and advanced knowledge in cyber security. The lab should provide students with active and project based learning in a real life cyber security environment. The students should be learning and applying cyber security techniques and tools to manage cyber security risks, to learn digital forensics, to get training on network forensics, and to handle incident response. These technical skills are critical for preventing successful cyber-attacks, improving cyber security, and maintaining trust in public and private institution to fortify security in the digital age. The increase in the number, sophistication, and complexity of cyber threats requires taking critical measures to equip students with the latest cyber security knowledge, skills, and research to have a future generation of professional experts in the area of cyber security. Therefore, each undergraduate cyber security program should create a community of cyber security professional experts and raise awareness of the critical role of cyber security in protecting public and private institutions and keep them safe.

2. PURPOSE OF CYBER SECURITY LAB AT UNDERGRADUATE INSTITUTION

First, creating cyber security lab should fill a gap in cyber security area by establishing a cyber security education and research lab at undergraduate institution. Second, the lab should be utilized as a resource to support and advance education and research at an undergraduate institution. Third, disseminate knowledge to students by adapting active and project based learning in a real life environment. Finally, conduct fundamental and applied research with undergraduate students and publish in regional and national conferences and in scholarly journals.

The objectives of building a cyber security lab should be of two-fold: education and research. Education should be achieved by providing knowledge and developing educational skills utilizing the cyber security lab to college students. The lab should be used to provide training to undergraduate students to help them understand and get interested in cyber security filed. This could be achieved by providing initial onsite training to students in cyber security and continue online training by granting remote access to the cyber security lab.

The research objectives should involve students directly in cutting-edge research; to give students the opportunity to learn and conduct research onsite and remotely through secure access to cyber security training and projects.

This approach should help undergraduate students to gain a significant practical experience of the concepts and practice of cyber security, to enhance their preparedness for employment to fill the speedily increasing number of jobs in this domain and create interest in postgraduate studies and research.

3. BACKGROUND LITERATURE

Cyber security is the mechanism of securing networks, computers, platforms, and pieces of information from illegal access, damage or any kind of attacks that intend exploitation. As of early August of 2017, applying cyber security as a keyword search to look for available jobs in USA recognized in excess of 11,000 in INDEED, more than 7,000 in LINK up, and over 1,000 jobs in Monster Jobs. The Workforce Intelligence Network for Southeast Michigan (WIN) [1] stated that there were about 350,000 cyber security-related job postings in USA between July 2015 and June 2016. Around 215,000 of these jobs (90%) require a bachelor degree or higher in cyber security or closely related area.

There is a huge need and demand for trained cyber security professionals. The Global Information Security Workforce Study in 2017 reported that more than 1.8 million cyber security positions globally will be unfilled by 2022 [2]. Forbes estimated that the cyber security market size will grow from $75 Billion in 2016 to $170 Billion by 2020 [3].
The hacking problem is becoming an epidemic. Fraley and Cannady [4] stated that "Malware by itself can represent as many as 3 million new samples an hour." McAfee Labs Threats Report that was issued on April 2017 shows that in 2016 the total number of new kinds of ransomware and malwares was more than 9 million and 600 million, respectively [5]. Figures 1-4 show the total number of new malware every three months and for the entire year of 2015 and 2016 [5].

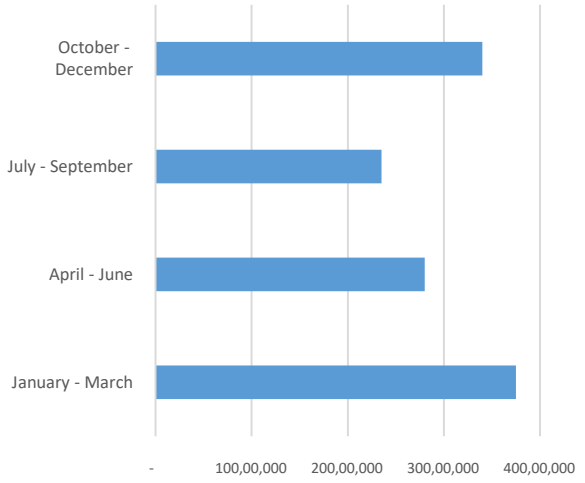

Fig1: Number of new Malware every three months in 2015

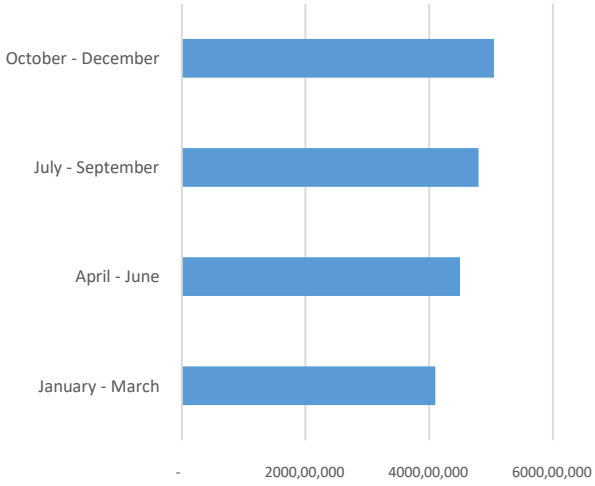

Fig2: Total number of new Malware in 2015

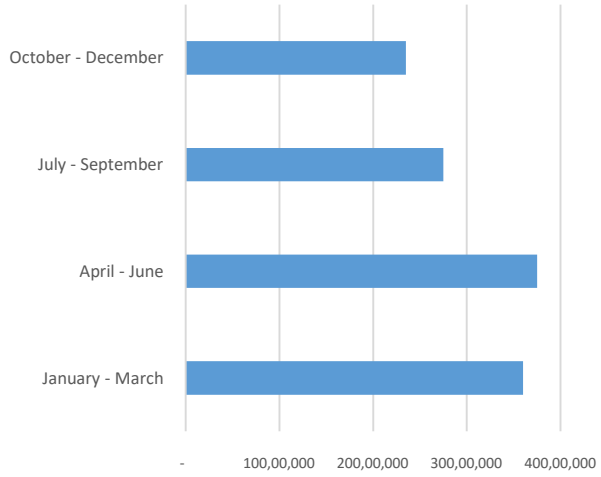

Fig3: Number of new Malware every three months in 2016

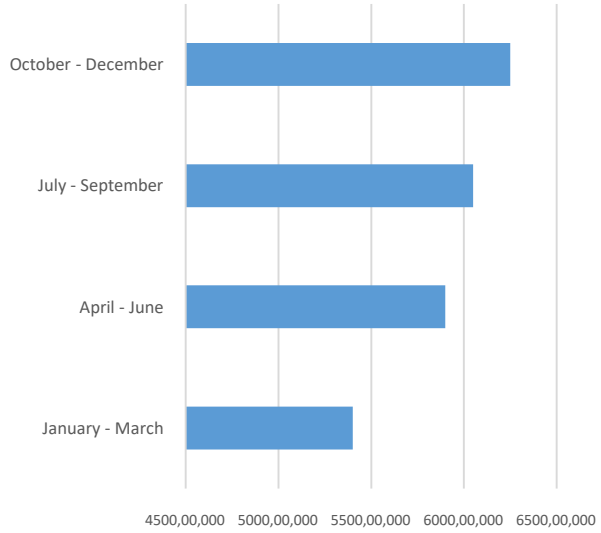

Fig4: Total number of new Malware in 2016

In May 2017, a ransomware attack infected more than 300,000 machines in more than 150 countries. The successful attacks enable ransomware hackers to lock access to the user data and demand money to unlock the data. Hackers were able to collect millions of dollars from their victims. Ransomware attack can be expanded beyond computers to target smartphones, tablets and likely anything connected to the Internet [3]. Figures 5-8 show the total number of new Ransomware every three months and for the entire year of 2015 and 2016 [5].

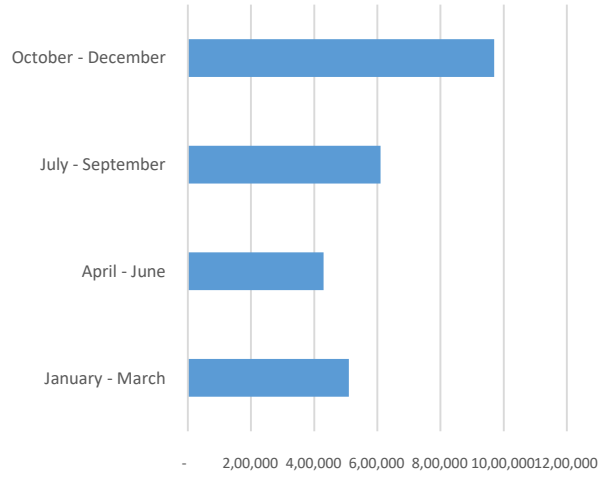

Fig5: Number of new Ransomware every three months in 2015

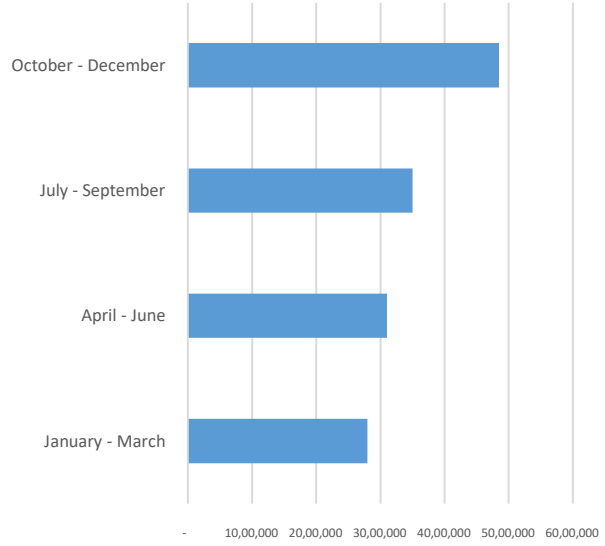

Fig6: Total number of new Ransomware in 2015

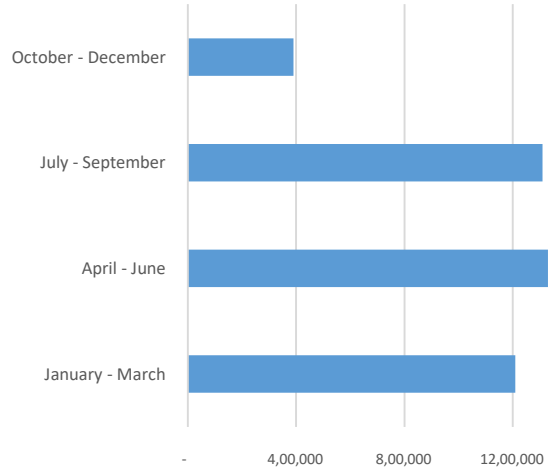

Fig7: Number of new Ransomware every three months in 2016

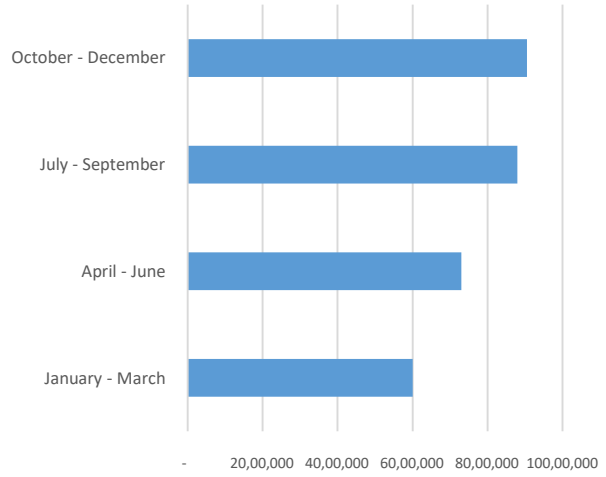

Fig8: Total number of new Ransomware in 2016

The problem we are facing daily is new and sophisticated malware that are currently in the making and have the ability to avoid network security infrastructures and perform attacks on the intended victims [4]. The Cisco 2017 Annual Cyber security Report [6] stated that more than one-third of institutions that have been subject to an attack suffered the loss of 20 percent of revenue or more. The challenges of increasing sophistication of data breaches, malware, and ransomware attacks is on the cybercrime top list of challenges for cyber security experts and law enforcement agencies.

Currently, the challenge is the high demand for fresh graduates with expertise in cyber security and it is a challenge to recruit students to continue their post graduate studies in the cyber security area.

There is a limited number of undergraduate institutions offering a cyber security as a minor and a very limited number of schools offering a cyber security as a standalone major. These majors involve little or no cyber security research.

Establishing cyber security lab should enhance and support college students in the highly demanded area of cyber security. The expectation that students should be able to develop a practical and professional knowledge of various aspects of cyber security and become active participants engaged in cyber security practice and research. Therefore, students should be either ready for professional practice in the area of cyber security at public and private institutions and/or pursue postgraduate studies and conduct cutting-edge research that will lead to measurable and lasting breakthrough in the area of cyber security.

The cyber security lab should trigger an interest in the research early on at undergraduate level by students involved in a real undergraduate research experience to build self-confidence and motivate students to pursue graduate studies and conduct a state-of-the-art cyber security research.

Students who will be involved in research-based investigations will appreciate the essence of scientific inquiry in cyber security in general and in understanding and analyzing data in particular. Establishing cyber security lab in undergraduate institution should support faculty to teach students to explore, develop and commence implementation of authentic cyber security research and to support both teaching and research in the area of cyber security for students at undergraduate level.

4. CONCLUSION

We believe establishing a cyber security educational and research training supported by a real life based lab environment will have lasting effect on the long-term trend both at an undergraduate cyber security program and in the cyber security workforce. Students will be trained to develop a practical and professional knowledge of various aspects of cyber security and to think critically and conduct research. Enhancing students' cyber security skills at an undergraduate cyber security program will lead to better equipped cyber security personnel. In addition, the lab can provide onsite cyber security training to students and continue online training by granting remote access to the lab.

REFERENCES

[1] Report: Demand for Cyber security Professionals Continues to Rise Across Michigan, Nationwide. 2017; Available from: http://www.dbusiness.com/daily-news/Annual-2017/Report-Demand-for-Cyber security-Professionals-Continues-to-Rise-Across-Michigan-Nationwide/.

[2] ISC2, The 2017 (ISC)2 Global Information Security Workforce Study. 2017.

[3] Morgan, S. One Million Cyber security Job Openings In 2016. Forbes. 2016; Available from: https://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cyber security-job-openings-in-2016/#f86601227ea2.

[4] Fraley, J.B. and J. Cannady. The promise of machine learning in cyber security. In SoutheastCon 2017. 2017.

[5] McAfee Labs Threats Report 2017.

[6] Cisco, 2017 Annual Cyber security Report. 2017.