Published by :
http://www.ijert.org

# Facilitating Regional Cybersecurity Workforce Development

Matthew A. Chapman,
Ph. D.
Assistant Professor of Information Technology
University of Hawaiʻi - West Oʻahu

***Abstract* – With growing cybersecurity workforce needs both regionally and globally, programs are required to develop information systems security professionals to meet these evolving requirements for stakeholders locally, nationally, and in the Asia-Pacific Region. The evolving programs at the University of Hawaiʻi - West Oʻahu are structured along two primary lines of effort to strengthen cyber workforce development; the implementation and expansion of a student-run cyber security coordination center and an increased cybersecurity focus on the protection of critical infrastructure.**

***Keywords—Cyber Workforce; Critical Infrastructure; SCADA; Cybersecurity***

## I. INTRODUCTION

Since 1976, the University of Hawaiʻi - West Oʻahu (UHWO) has served the people of Hawaiʻi and remains a dynamic and diverse place of learning and cultural enrichment. UH West O'ahu is located in the city of Kapolei on the island of O'ahu, and is a four-year, comprehensive university with an emphasis on career-related baccalaureate education based on state, regional, and global needs. The university is located closely to key defense and military facilities to include Joint Base Pearl Harbor-Hickam, Headquarters United States Pacific, Command, Schofield Barracks, Kaneohe Marine Corps Base, and numerous critical infrastructure facilities [1].

Based on the rapid expansion of cyberspace operations and the importance of cyber security to both the government and industry, UHWO developed the Bachelor of Applied Science degree with a concentration in Information Security and Assurance (BAS-ISA). This degree program is the first of its kind at a public institution in Hawaiʻi and the Pacific, developed in response to state, national and regional needs for graduates with education in information security. The concentration was developed in cooperation with Honolulu Community College, state and federal law enforcement agencies, state security officials, and local businesses, and covers a wide variety of technical and managerial aspects within the field.

The Committee on National Security Systems has certified that the University of Hawaiʻi - West Oʻahu offers a set of courseware meeting national training standards for information systems security professionals. In order to meet workforce development needs on Oʻahu, nationally, and in the Asia-Pacific Region, the BAS-ISA program plans to further distinguish its strengths in both information assurance and cyber security to meet these expanding cybersecurity workforce needs [2]. The objective of this expansion is to meet emerging requirements for information security professionals, while aligning directly with the mission and vision of the program as stated below:

> *"Prepare Native Hawaiian, local, and regional students for employment in the information technology and information security career fields upon graduation (Mission)."*
>
> *"Establish and expand the UHWO Cyber Security Coordination Center as a center of academic excellence in information security and cyber defense, educating students to be engaged global citizens and leaders in our society (Vision)."*

Additionally, personnel reporting highlights plans to develop a robust workforce of cyberspace professionals to man critical positions. This reporting identifies personnel shortfalls that may directly increase opportunities for professionals entering the cybersecurity workforce [3].

Expansion of the ISA program to meet expanding requirements is structured along two primary lines of effort. They are presented here to offer a framework to facilitate the expansion of cyber workforce development programs.

## II. DEVELOPMENT AND EXPANSION OF THE UHWO CYBER SECURITY COORDINATION CENTER (CSCC)

The purpose of the UHWO CSCC is to support cyber workforce development needs by providing students with the opportunity to work in a cyber operations center and coordinate cyber defense information with local and regional partners. This center provides students with experience and education as network defense subject matter experts in order to prepare them for future employment. The experience is directly related to needs in industry and other organizations requiring information security expertise.

The CSCC also supports information security needs in the community and region by acting as a resource to learn about modern cyber conflicts and emerging cyber threats. Curriculum courses that support this center include courses in secure software programming, proactive system security, digital forensics, management of information security, information technology project management, modern cyber conflicts, and senior capstone research courses [4].

Students are afforded the opportunity to put coursework to practical use in the CSCC, better preparing them to enter the cyber workforce. As described in *Planning for Malicious Activity on Communications Networks* [5], Significant considerations in planning for malicious activity include monitoring developments in the global cyberspace environment, monitoring the technical cyberspace environment as new vulnerabilities are discovered, conducting digital forensics, and implementing best practices for information security.

### A. *Monitoring the Global Cyberspace Environment*

Monitoring the global cyberspace environment requires the student analyst to research strategic actors, emerging operations, and developments in policies relating to the global cyberspace environment through the use of open source resources. Some of these developments are likely to influence business decisions and strategies, as well as national and regional policy.

The responsibilities of the global cyber environment analyst, as listed on the CSCC portal, include keeping up to date on the global cyber environment, producing weekly executive summaries, and maintaining the aggregation of information on the CSCC portal [6].

### B. *Technical Developments and Vulnerabilty Analysis*

As it is important to monitor the global cyberspace environment at the strategic and operational levels, it is also critical to monitor recent developments at the technical level, specifically the latest system vulnerabilities.

The responsibilities of the vulnerability research analyst include the tracking of current security bulletins, the collection of open source notifications concerning vulnerabilities for local and regional awareness, the development of a weekly summary, and maintenance of the vulnerabilities section of the CSCC web portal [7].

### C. *Digital Forensics*

The Digital Forensics Analyst leverages skills and knowledge gained from coursework to expand digital forensics research and gain experience working in an operations center. Both networked and stand-alone systems should be available to test technical developments and vulnerabilities relayed from the vulnerability analyst.

The responsibilities of the digital forensics analyst include identifying artifacts, analyzing information, and facilitating research information on digital forensics through the CSCC web portal [8].

### D. *Best Practices*

As one of the key functions of the UHWO CSCC is to coordinate cyber defense information with local and regional partners, the best practices analyst has the responsibility to publicize best practices for information security. This is a complex task that requires the analysist to stay abreast of the developments in the cyber environment strategically, operationally, and technically, providing best practices for partners to leverage, in order to increase their security posture.

The responsibilities of the best practices researcher is to provide updates on the CSCC portal pertaining to security solutions that may include software upgrades and patches, network and host security solutions, and a weekly summary of developments [9].

## III. Focus on the Protection of Critical Infrastructure

Recent events have highlighted the importance of cybersecurity relating to the protection of critical infrastructure, specifically the prolonged blackout in the Ukraine reported in December, 2015. This attack reportedly caused a major power outage by disconnecting electrical substations. It seems increasingly important to provide the future cybersecurity workforce with experience working with systems and protocols used in critical infrastructure or industrial control systems (ICS) [10] [11].

Systems that monitor and control ICS networks are referred to as supervisory control and data acquisition (SCADA) system. SCADA systems are commonly found controlling electrical utilities, power companies, water companies, and mass transit facilities. SCADA refers to telemetry and data acquisition, and includes the collection of information from remote terminal units (RTU) by a master control station [12].

The protocols commonly involved in communications between master control stations and RTUs generally vary from the TCP/IP protocol taught in traditional networking and information security courses. In order to specifically focus on future cyber workforce needs, it is increasingly important to introduce protocols involved in ICS communications to undergraduate students. This will make the student more competitive to enter the workforce, but more importantly, start more information security professional on the path to ICS cybersecurity [12].

The main programs involved in increasing focus on ICS cybersecurity are the introduction of additional coursework and the establishment of ICS simulations for student familiarization.

### A. *Development of New Coursework*

The first aspect of this two-pronged program to focus on ICS cybersecurity is curriculum development. For the BAS-ISA program, the result was an approved course titled, "*Cybersecurity for Supervisory Control and Data Acquisition (SCADA) Systems.*" This course will explore the fundamentals of SCADA network architecture and associated communication protocols. The topics covered include ICS, embedded systems, and hardware security.

This additional coursework in concert with established programs and industry standard knowledge areas in information security, will help provide the foundational knowledge for further research and employment related to ICS cybersecurity.

### B. *ICS Simulations*

The objective of lab simulations is to provide students the opportunity to observe and research commands related to SCADA communications. The UHWO CSCC established a simulation to facilitate familiarization of common ICS protocols, here specifically focusing on the Distributed

Network Protocol (DNP3); although, other common protocols, such as the International Electrotechnical Commission (IEC) 60870 are also quite applicable. The UHWO CSCC critical infrastructure lab is built around the Triangle Microworks Test Harness software, allowing students to view the traffic between master and remote stations with a customizable protocol analyzer [13]. These simulations should supplement coursework to support cyber workforce development focusing on ICS cybersecurity.

## IV. CONCLUSION

With growing cybersecurity workforce needs both regionally and globally, programs are required to develop information systems security professionals to meet these evolving requirements for stakeholders locally, nationally, and in the Asia-Pacific Region. Information security programs may consider expanding efforts along two primary lines of effort to strengthen cyber workforce development, the implementation of a cyber security coordination center and an increased focus on the protection of critical infrastructure. Key areas of research for a student-run cyber security coordination center are researchers focused on the global cyberspace environment, vulnerability research, digital forensics, and information security best practices. Key areas of implementation for an increased focus on ICS cybersecurity include developing new curriculum and the integration of SCADA simulations.

## ACKNOWLEDGMENTS

Thank you to the faculty and staff of the University of Hawaiʻi - West Oʻahu for your support and Aloha. A special Mahalo to the first student interns at the UHWO CSCC, Melvin Quemado, Edward Chang, John Atienza, Taylor Sakuda, and Jerry Adams for your hard work bringing the center to life. You have a bright future as information security professionals.

## REFERENCES

[1] University of Hawaii. “About UHWO”. University of Hawaii West Oahu, . [Online]. Available: http://www.uhwo.hawaii.edu/about-us/. [Accessed 17 12 2014].

[2] National Security Agency, Central Security Service, "National Centers of Academic Excellence in Information Assurance (IA)/Cyber Defense (CD)," 2014. [Online]. Available from: https://www.nsa.gov/ia/ [Accessed 15 12 2014].

[3] Department of the Navy, "CNO's Position Report," Washington D.C., 2014.

[4] University of Hawaii. General Catalog 2014-2015 [online]. Kapolei, HI: Univerity of Hawaii West Oahu, 2015. Available from www.uhwo.hawaii.edu/general-catalog/ [Accessed 07 04 2015].

[5] M. Chapman (2015). “Planning for Malicious Activity on Communications Networks”. International Journal of Engineering Research & Technology (IJERT), Vol. 4 Issue 09.

[6] UHWO CSCC. “Global Cyber Envirnment”. Available from ww.uhwo.hawaii.edu/cyber/global-cyber-environment.

[7] UHWO CSCC. “Vulnerability Research”. Available from ww.uhwo.hawaii.edu/cyber/vulnerability-research.

[8] UHWO CSCC. “Forensic Inverstigations”. Available from http://www.uhwo.hawaii.edu/cyber/index.php/forensic-investigations/.

[9] UHWO CSCC. “Best Practices”. Available from http://www.uhwo.hawaii.edu/cyber/index.php/best-practices/.

[10] K. Granville (2015, February 5). “9 Recent cyberattacks against big business”. The New Your Times [online]. Available from www.nytimes.com/interactive/2015/02/05/technology/recent-cyberattacks.html?_r=0 [Accessed 10 09 2015].

[11] P. Paganini (2016, January 12). “Black Energy Used as a Cyber Weapon Against Ukranian Critical Infrastructure”. Infosec Institute [online]. Available from http://resources.infosecinstitute.com/blackenergy-used-as-a-cyber-weapon-against-ukrainian-critical-infrastructure/.

[12] G. Clark and D. Reynders. Practical Modern SCADA Protocols. Newnes, Burlington, MA., 2006.

[13] Triangle Microworks. “Testing and Configuration Tools”. Available from www.trianglemicrowork.com.