Kennesaw State University
DigitalCommons@Kennesaw State University

Faculty Publications

1-1-2013

Addressing Emerging Information Security Personnel Needs. A Look at Competitions in Academia: Do Cyber Defense Competitions Work?

Andrew Green
Kennesaw State University

Humayun Zafar
Kennesaw State University

Follow this and additional works at: https://digitalcommons.kennesaw.edu/facpubs

Recommended Citation
Green, Andrew and Zafar, Humayun, "Addressing Emerging Information Security Personnel Needs. A Look at Competitions in Academia: Do Cyber Defense Competitions Work?" (2013). *Faculty Publications*. 4281.
https://digitalcommons.kennesaw.edu/facpubs/4281

This Article is brought to you for free and open access by DigitalCommons@Kennesaw State University. It has been accepted for inclusion in Faculty Publications by an authorized administrator of DigitalCommons@Kennesaw State University. For more information, please contact digitalcommons@kennesaw.edu.

Addressing Emerging Information Security Personnel Needs. A Look at Competitions in Academia: Do Cyber Defense Competitions Work?

Research-in-Progress

Andrew Green
Kennesaw State University
agreen57@kennesaw.edu

Humayun Zafar
Kennesaw State University
hzafar@kennesaw.edu

ABSTRACT (REQUIRED)

This paper is part of a proposed study that looks at the emerging information security personnel needs of organizations. We are attempting to explore the correlation between components of a regional cyber defense competition and an organization's needs in terms of employing adequately trained information security personnel. We look to identify some unique characteristics of a regional academic cyber defense competition via the critical success factors method.

Keywords (Required)

Pedagogy, academia, competition, benefits, cyber defense

INTRODUCTION

We routinely witness events that highlight the need for a strong information security (infosec) infrastructure. Even in tough economic times, investments in infosec related ventures are projected to rise (Benner 2013). Infrastructure has been a hot infosec topic over the last several years. Virtualization, mobile, and supervisory control and data acquisition (SCADA) are among the various infrastructure types which have captured much attention regarding how they impact the way security is viewed. A buzz term of 2012 - "big data"- which can represent many different ideas depending on what the data is, has also appeared on the horizon. In the infosec industry, enterprises want to enable better security decisions based on their security data. The apparent need for more actionable information implies a need for actionable defenses to take advantage of this data (Davis Gragido Hein Hils Holden Jagdale Jones Lake Lancaster Painter Park Pirc Quinlan Sechman Shah Smith Thuma and Timpe 2011). Considering that organizations are faced with these challenges, which are numerous today and will only grow in the future, ensuring that an appropriate human resource is available becomes important. Therefore, it is not a surprise that infosec has grown as a career choice. There has been a corresponding increase in institutional support for higher education in the area, as evidenced by the increasing numbers of institutions recognized by the Department of Homeland Security (DHS) and the National Security Agency (NSA)'s joint program: National Centers of Academic Excellence in Information Assurance Education (NCAE/IAE). DHS and NSA work cooperatively to fill a widely perceived need for increased numbers of infosec professionals in both the public and private sectors, and have been mandated to support the development of infosec professionals by supporting public education efforts. Part of this support has resulted in the creation of regional cyber defense competitions, winners of which meet at a national event. One of the main reasons behind their creation is to prepare the infosec workforce of the future. We plan to investigate in depth once such event, the Southeast Collegiate Cyber Defense Competition (SECCDC). The Southeast Collegiate Cyber Defense Competition (SECCDC) is a regional qualifier event for the National Collegiate Cyber Defense Competition (CCDC). The CCDC is billed as "…a three day event and the first competition that specifically focuses on the operational aspect of managing and protecting an existing 'commercial' network infrastructure (n.d.).

Using the critical success factor method (CSF) (Bullen and Rockart 1981; Rockart 1979), we intend to identify some of the unique factors from a participant's (student) viewpoint, and compare them against industry demands. Are we truly preparing the infosec professional of the future? Or do we, as academics, need to get a better grasp of what external threats organizations are facing now, as well as what they expect to face in the future?

LITERATURE REVIEW

A review of the literature highlights the lack of exploration regarding the benefits to students from cyber defense competitions that are not otherwise available to them through other competitions.

Existing literature has examined the structure of cyber defense competitions (Dodge and Ragsdale 2004; Schepens and James 2003). Other literature has examined how the use of cyber defense competitions has been used to shape curriculum (Conklin 2005, 2006; Mullins Lacey Mills Trechter and Bass 2007; Schweitzer Gibson and Collins 2009). (Hoffman Rosenberg Dodge and Ragsdale 2005) examined structural and resource-related issues associated with staging a cyber defense competition. (Mattson 2007) examined how to offer cyber defense competitions in the private sector, using a service provider model. Other literature has examined the benefit of conducting cyber defense competitions at the K-12 level (Rursch Luse and Jacobson 2010; White Williams and Harrison 2010).

SECCDC OVERVIEW

The SECCDC is hosted at Kennesaw State University (KSU), located in Kennesaw, Georgia. The competition has grown in size over the last 7 years. For the first time, in 2013, event organizers had to stage a "virtual qualifier" in order to determine the top eight teams that would advance to the onsite competition held on the KSU campus.

In keeping with the spirit of the CCDC, the SECCDC creates identical networks, client systems, and servers for the teams to use, in both the "virtual qualifier" as well as the onsite competition. These networks are identified as being different divisions of Hierarchical Access Limited (HAL), a fictional organization. The scenario holds that the student teams are being brought in to replace the previous IT staff, which was fired due to incompetence.

The client systems, servers, and networking equipment are misconfigured to varying degrees, and contain varying types of operating systems. The typical list of operating systems includes a mix of Windows Servers (2003 and 2008), various Linux distributions (CentOS, Ubuntu, Red Hat Enterprise, FreeBSD, Fedora Core, and Debian), as well as Windows client operating systems (2000, XP, 7, and 8). Additionally, software-based firewall distributions have been used in previous competitions (Vyatta, pfSense, Untangle, Smoothwall).

These various systems have been pre-configured to offer various services that are deemed critical to the day-to-day functionality of HAL. In past competitions, these services have included web sites (both hypertext transfer protocol (HTTP) and hypertext transfer protocol secure (HTTPS)), simple mail transfer protocol (SMTP), database services, and domain name system (DNS) services. The challenge to the teams is to normalize the existing systems to the best of their ability, while responding to HAL management requests for common business tasks, or injections. Injections can range from adding/removing employees, to making new services available, to adding or removing hardware to or from the environment. All of this is being done while the networks are under constant attack from professional penetration testers. The student teams are expected to defend their network from compromise, while ensuring critical services are kept functional, while also responding to the demands of injections as they come in from the HAL corporate entity.

CRITICAL SUCCESS FACTORS

According to Rockart (1979), CSFs are things that must go well to ensure success in an organization. CSFs are extracted via the CSF method. In the field of information systems (IS) research, Rockart introduced the CSF method as a mechanism for aligning information technology (IT) planning with the strategic direction of an organization. In the CSF method, an analyst and key personnel of an organization take part in a dialogue. Initial CSFs are extracted from that meeting, and the analyst presents them in detail to the same personnel again. This process continues until a satisfactory list of CSFs has been identified. This dialogue generates user acceptance, as most seem to intuitively understand the thrust of the CSF method, and therefore endorse its usage as a means of identifying areas of concern in an organization (Boynton and Zmud 1984). Rockart (1979) presented service, communication, human resources, and repositioning the IS function as generic CSFs. He noted that while specific CSFs would differ from one participant to another, the generic set was readily apparent in the companies that were studied. In this study, we plan to validate the use of all the generic CSFs that Rockart presented, while attempting to extract new CSFs pertaining directly to the study.

We intend to apply the CSF method in an in-depth study at the SECCDC. Precedence for using the CSF approach in a single organization or event in different contexts has been set (Shank Boynton and Zmud 1985; Slevin Stieman and Boone 1991). We plan to ascertain some of the learning outcomes of the SECCDC for students at different stages of their degree program. Precedence of a multi-layered CSF study has been set. Bullen and Rockart (1981) researched layers of management. We also plan to go one step further and include the administrative layer as well.

Research Model

Using the concepts outlined in the CSF methodology, we have constructed an initial research model. This model shows the CSFs as dependent variables (DV), and their relationship to the traits exhibited by a successful infosec worker.

Proposed Research Model

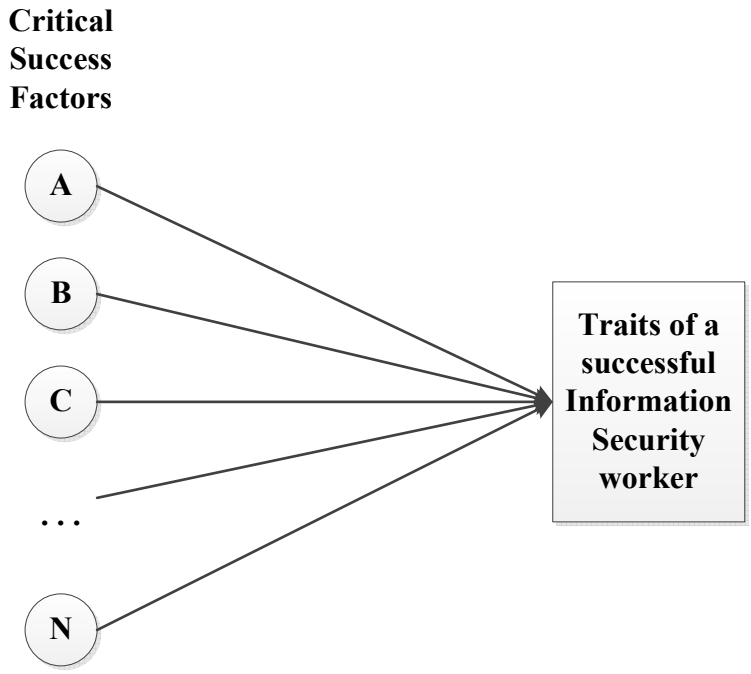

Figure 1

The CSFs will be identified in the future, after we are able to identify and interview appropriate subjects in order to collect the necessary data.

SURVEY CREATION

Once CSFs have been synthesized, we plan to create a survey that will have multiple Likert based items pertaining to each CSF. It will be sent to organizations that have been a part of SECCDC. This will allow us to adjudicate on some of the characteristics of SECCDC, and to ascertain if the competition is addressing industry concerns. Due to the nature of our relationship with various organizations, we do not foresee an issue with getting enough data for validation and analysis.

CONTRIBUTIONS TO INDUSTRY AND ACADEMIA AND CONCLUSION

There are many potential benefits to industry and academia from this study. CSFs identified in this study could be used by competition administrators to help shape future SECCDC competitions. By extension, a better competition will assist in preparing students for their career fields. This would also ensure that the competition stays relevant and current in terms of challenges being presented to competing teams. These same CSFs could also be used by instructors to help guide learning outcomes and objectives for courses being taught, or could be used to assist in the development of new courses.

Soliciting input from industry on the identified CSFs could be used to validate the list, help industry understand what potential future employees identify as factors critical for their success, as well as possibly discovering additional CSFs not

identified by the original study. These additional CSFs could then be used by competition administrators to help shape the nature and scope of the competition, thus helping to better prepare students for positions in industry. These same CSFs could also be used to help guide learning outcomes and objectives for courses being taught, or could be used to assist in development of new courses.

We would like to use this platform to get a sense of some of the recommendations academics and practitioners may have about our approach.

REFERENCES

1. "Competiton Overview," National Collegiate Cyber Defense Competition, n.d.

2. Benner, K. "Cyberdefense: A new opportunity for investors," 2013.

3. Boynton, A., and Zmud, R. "An assessment of critical success factors," *Sloan Management Review (pre-1986)* (25:4) 1984, pp 17-27.

4. Bullen, C.V., and Rockart, J.F. "A primer on critical success factors," Massachussets Institute of Technology, pp. 1-64.

5. Conklin, A. "The Use of a Collegiate Cyber Defense Competition in Information Security Education," in: *2nd Annual Conference on Information Security Curriculum Development*, Association of Computing Machinery, Kennesaw, Georgia, 2005, pp. 16-18.

6. Conklin, A. "Cyber Defense Competitions and Information Security Education: An Active Learning Solution for a Capstone Course," 39th Annual Hawaii International Conference on System Sciences, Honolulu, Hawaii, 2006, pp. 1-6.

7. Davis, L., Gragido, W., Hein, B., Hils, A., Holden, D., Jagdale, P., Jones, J., Lake, J., Lancaster, J., Painter, L., Park, Y., Pirc, J., Quinlan, E., Sechman, J., Shah, N., Smith, C., Thuma, M., and Timpe, J. "2011 top cyber security risks report," 2011.

8. Dodge, R.C., and Ragsdale, D.J. "Organized Cyber Defense Competitions," IEEE International Conference on Advanced Learning Technologies, 2004, pp. 768-770.

9. Hoffman, L.J., Rosenberg, T., Dodge, R., and Ragsdale, D. "Exploring a national cybersecurity exercise for universities," *IEEE Security & Privacy Magazine* (3:5) 2005, pp 27-33.

10. Mattson, J.A. "Cyber Defense Exercise: A Service Provider Model," in: *Fifth World Conference on Information Security Education,* L. Futcher and R. Dodge (eds.), Springer, 2007, pp. 81-86.

11. Mullins, B.E., Lacey, T.H., Mills, R.F., Trechter, J.M., and Bass, S.D. "How the Cyber Defense Exercise Shaped an Information-Assurance Curriculum," *IEEE Security & Privacy Magazine* (5:5) 2007, pp 40-49.

12. Rockart, J.F. "Chief executives define their own data needs," *Harvard Business Review* (57:2) 1979, pp 81-93.

13. Rursch, J.A., Luse, A., and Jacobson, D. "IT-Adventures: A Program to Spark IT Interest in High School Students Using Inquiry-Based Learning With Cyber Defense, Game Design, and Robotics," *IEEE Transactions on Education* (53:1) 2010, pp 71-79.

14. Schepens, W.J., and James, J.R. "Architecture of a Cyber Defense Competition," IEEE International Conference on Systems, Man and Cybernetics, IEEE, 2003, pp. 4300-4305.

15. Schweitzer, D., Gibson, D., and Collins, M. "Active Learning in the Security Classroom," 42nd Hawaii International Conference on System Sciences, Honolulu, Hawaii, 2009, pp. 1-8.

16. Shank, M.E., Boynton, A.C., and Zmud, R.W. "Critical success factor analysis as a methodology for MIS planning," *MIS Quarterly* (9:2) 1985, pp 121-129.

17. Slevin, D.P., Stieman, P., and Boone, L. "Critical success factor analysis for information systems performance measurement and enhancement. A case study in the university environment," *Information & Management* (21:3) 1991, pp 161-174.

18. White, G.B., Williams, D., and Harrison, K. "The CyberPatriot National High School Cyber Defense Competition," *IEEE Security & Privacy Magazine* (8:5) 2010, pp 59-61.