ISSN: 2473-4901
v5 n4954

A Survey on CISSP (Certified Information Systems Security Professional) Contributions to Higher Education Research

Randy Brown
rwbrown@tamuct.edu
Texas A & M Central Texas

Abstract

An increasing awareness of Information and Cyber Security threats has led to higher numbers of students seeking security related curriculum. Higher Education is responding with security related programs and seeking certified instructors, often CISSPs, for those programs. As both professionals and educators, CISSPs have multiple responsibilities to both the profession and education. This raises some questions about how CISSPs in Higher Education are expected to contribute to the Information Security Body of Knowledge. Should academic CISSPs contribute security related research to the academic body of knowledge? What percentage of their research should CISSPs devote to security related research? This study investigates these questions and others through a small survey asking CISSPs their opinions about contribution expectations to Higher Education research. The results suggest CISSPs should contribute at least some security related research.

Keywords: CISSP, Information Security, Security Education, Cyber Security

1. INTRODUCTION

As awareness of information and cyber threats increase, more students seek degrees related to Information or Cyber Security. To meet this need, many educational institutions are adding security related programs, and are seeking qualified and or certified instructors to teach the courses (Bicak, Liu, & Murphy, 2015; Martin & Woodward, 2013). This seems to be especially true for institutions who have obtained or are seeking status as NSA approved Centers of Academic Excellence in Cyber Operations or Defense (O'Neil, 2013; Yang & Wen, 2017).

There are a number of certifications in high demand, including, but not limited to, Certified Ethical Hacker (CEH), Certified Information Security Manager (CISM), CompTIA Security+, CISSP: Certified Information Systems Security Professional, and GSEC: SANS GIAC Security Essentials (Brown, 2019; McLaughlin, 2005; Walters, 2007). This particular study focuses only on CISSP.

The CISSP has highly rigorous standards for achieving and maintaining the certification. According to the $(ISC)^2$, the certifying organization for the CISSP and other security certifications, a CISSP should:

- Protect society, the common good, necessary public trust and confidence, and the infrastructure.
- Act honorably, honestly, justly, responsibly, and legally.
- Provide diligent and competent service to principles.
- Advance and protect the profession

"CISSP – The World's Premier Cybersecurity Certification," 2019). The important tenet for this study is the last, "Advance and protect the profession". While there may be numerous ways to accomplish this, contributing to professional and academic bodies of knowledge is the focus of this study.

Specific publication requirements are dependent upon the type of organizations, but the general expectation across all of them is "publish or perish." In many higher education organizations jobs, tenure, and promotion are often driven by

whether the academic produces publications. For Centers of Academic Excellence (CAE) research in the security area is essentially required by the NSA as part of the requirements for a CAE (NSA, 2019). The requirement for the CISSP to contribute to the profession combined with the requirements of academia leads to a discussion about whether CISSPs in higher education should produce publications that are related to security (Brown, 2019; Walters, 2007; Yang & Wen, 2017).

This study is an attempt to provide some initial perspectives on the question about how CISSPs should contribute to higher education. To answer this question, we utilized a survey to ask CISSPs who have published in higher education journals about their perceptions.

2. SURVEY DEVELOPMENT AND IMPLEMENTATION

The survey was very short and very open-ended with questions aimed at addressing the level of contribution of the CISSP to higher education. The first few questions focused on demographics and included statistics about when the CISSP certificate was awarded, when the author entered academia, publication contributions since obtaining CISSP, whether the author contributed in some way to a security related curriculum, etc. The full set of survey questions is available in the appendices.

The primary question was what ratio of security to non-security related publications should be expected by a CISSP in higher education. This was a seven point Likert scale ranging from none of the articles needed to by security related to all needed to be security related. The question was followed by an open-ended question on why the respondent felt the way he/she did. The final question was another open ended question simply asking for any additional comments the respondent might have.

The next step was selecting the target audience. While this seemed simple, in implementation it proved a bit challenging. Utilizing online databases of academic publications, a list of CISSP designated authors was collected. The databases include were Academic Search Premier, ProQuest, JSTOR, EBSCO Host, and Business Source Complete. Obviously these are not all-inclusive of the possible outlets for CISSP authors, but they are a good place to start.

A list of 77 authors with CISSP designations was compiled. Attempts to locate viable contacts for these 77 authors resulted in 45 working email addresses, all of whom were invited to participate in the survey. Twelve invitees responded (26%) to at least some of the questions. Nine (20%) completed all questions. While this number is low, it can still be useful for providing useful perspectives. Other studies have shown that, historically, online surveys tend to have lower response rates (Kongsved, Basnov, Holm-Christensen, & Hjollund, 2007; Poynton, DeFouw, & Morizio, 2019). While there is some research into improving the response rate (Kent & Brandal, 2003; Pedersen & Nielsen, 2016; Wright & Schwager, 2008), they were not incorporated into this pilot study, but could be incorporated into future research.

3. SURVEY RESULTS AND ANALYSIS

Examining the respondents' demographic information, we find a good cross-section of authors. The respondents were from academics throughout the world, from both academic and professional settings, with most being from the United States. While most were academics, some were professionals in industry positions.

Most of the respondents attained CISSP certification prior to 2005. The most recent was 2011. This might be something to investigate further with an extended survey. Total number of articles published ranged from one to more than twenty. Note that not all publications were security related, but all were post author CISSP certification status.

Seven of respondents indicated they were contributed to security curriculum of some kind, including centers for excellence. Two respondents were not, the remainder did not respond to this question.

Figure 1 shows the distribution of the nine responses related to the ratio of Security related to non-security related publications. Most felt that at least some of the publications produced by a CISSP should be Security related. A follow-on question asking the respondents to explain their response further back up these results. Even the respondent who indicated none were required indicated in other comments that Security related articles were important.

Explanations of why the respondents answered the above question as they did were varied, but the common thread was still academics, including CISSPs, should produce research related to their areas of academic concentration. Some of the

ISSN: 2473-4901
v5 n4954

responses were quite interesting and have been included in the Appendixes.

The final question was open-ended to allow the respondents to add any additional comments about the topic, the survey, etc. While most were not really related to the survey, some provided additional thoughts about what areas CISSPs, and other academics, should publish. Some of the comments are included in the Appendixes.

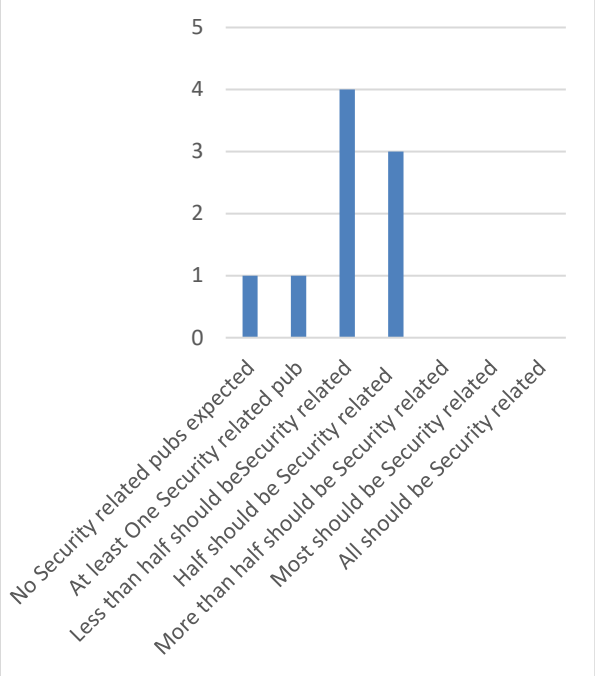

Figure 1: Ratio of Security vs non-Security Related Publications

4. CONCLUSIONS

This study has attempted to build on the question of CISSP contribution to higher education research. There are several limitations to this study. First is the small number of respondents. There were only twelve responses of which only nine completed all questions. While there are enough for a pilot study, more respondents would be necessary to really portray industry-wide expectations. Second is the way the CISSPs names and contact information were gathered. Only those who have published articles in the journals represented by those databases who included their CISSP designation would have been located. Third, the survey was very subjective, there were qualitative questions. This could lead to some ambiguity, but considering the goals of the survey, this was felt to be appropriate.

In spite of the limitations, this study has provided some valuable insights into the opinions of CISSPs currently contributing to higher education research about the types or areas in which academic CISSPs should be contributing. One major consistency found during this study is that the expectation for the CISSP in academia is to produce at least some research related to security, but should also contribute in other areas in which the academic CISSP is involved.

Another finding is that this dialog is of interest to several of the CISSPs who participated and has been of interest for several years, even decades as one respondent indicated. There were additional comments for additional areas of study related to Information Security.

From the results of this pilot study, the discussion about how CISSPs should be expected to contribute is of some interest to the community and should be expanded and continue. At the least, it should encourage academic CISSPs to consider how they are contributing to academic research.

5. REFERENCES

Bicak, A., Liu, M., & Murphy, D. (2015). Cybersecurity Curriculum Development: Introducing Specialties in a Graduate Program. *Information Systems Education Journal, 13*(3), 99-110.

Brown, R. (2019). The Contribution of the CISSP (Certified Information Systems Security Professional) to Higher Education Research. *Information Systems Education Journal, 17*(3), 5.

CISSP – The World's Premier Cybersecurity Certification. (2019). Retrieved from https://www.isc2.org/Certifications/CISSP

Kent, R., & Brandal, H. (2003). Improving email response in a permission marketing context. *International Journal of Market Research, 45*(4), 489-503. doi:10.1177/147078530304500404

Kongsved, S. M., Basnov, M., Holm-Christensen, K., & Hjollund, N. H. (2007). Response rate and completeness of questionnaires: A randomized study of Internet versus paper-and-pencil versions. *Journal of Medical Internet Research, 9*(3), p39-p48. doi:10.2196/jmir.9.3.e25

ISSN: 2473-4901
v5 n4954

Martin, N., & Woodward, B. (2013). Building a Cybersecurity Workforce with Remote Labs. *Information Systems Education Journal, 11*(2), 57-62.

McLaughlin, L. (2005). Cybercorps Scholarships Fund New Generation of Security Gurus. *IEEE Software, 22*(1), 98-100. doi:10.1109/MS.2005.11

NSA. (2019). CAE REQUIREMENTS AND RESOURCES. Retrieved from https://www.iad.gov/nietp/CAERequirements.cfm

O'Neil, M. (2013). U.S. Agencies Revamp Standards for Cybersecurity Program. *Chronicle of Higher Education, 60*(5), A18-A19.

Pedersen, M. J. m. s. d., & Nielsen, C. V. (2016). Improving Survey Response Rates in Online Panels. *Social Science Computer Review, 34*(2), 229-243. doi:10.1177/0894439314563916

Poynton, T. A., DeFouw, E. R., & Morizio, L. J. (2019). A systematic review of online response rates in four counseling journals. *Journal of Counseling & Development, 97*(1), 33-42. doi:10.1002/jcad.12233

Walters, L. M. (2007). A Draft of an Information Systems Security and Control Course. *Journal of Information Systems, 21*(1), 123-148.

Wright, B., & Schwager, P. H. (2008). Online Survey Research: Can Response Factors Be Improved? *Journal of Internet Commerce, 7*(2), 253-269. doi:10.1080/15332860802067730

Yang, S. C. s. f. e., & Wen, B. (2017). Toward a cybersecurity curriculum model for undergraduate business schools: A survey of AACSB-accredited institutions in the United States. *Journal of Education for Business, 92*(1), 1-8. doi:10.1080/08832323.2016.1261790

Appendices

A-1: Survey Questionnaire

1. Demographics
   - 1a. Name
   - 1b. Academic Affiliation (school)
   - 1c. Academic Rank
   - 1d. Date of CISSP activation
   - 1e. Date entered Academia
2. Are you involved in a security specific curriculum? (Yes/No)
   - 2a. If so, please describe your program.
3. Please list your publications AFTER obtaining CISSP
4. What publication expectations do you have concerning the academic contributions of CISSP's in Higher Academic positions, with respect to Info Sec related articles vs. non-Info Sec articles?

   Seven Point Likert Scale:

   i. No publications need to be Information Security Related
   ii. Only one publication needs to be Information Security Related
   iii. Less than half of publications need to be Information Security Related
   iv. Half of publications need to be Information Security Related
   v. More than half of publications need to be Information Security Related
   vi. Most (all but one) publications need to be Information Security Related
   vii. All publications need to be Information Security Related
5. Please provide any other thoughts you might have concerning the contribution of CISSPs to Higher Education research.

A-2: Selected Comments to Question 2a (See A-1, above)

Note: For confidentiality, respondent identifying information may have been removed.

"I believe an information security professional should be well-rounded from an experience and knowledge perspective."

"I have argued for decades that information assurance MUST be based on a broad perspective, not a narrowly technical one."

"The ratio should be specific to the research interests of the academic."

"It is what the academic DOES, not what he/she writes that counts."

A-3: Selected Comments to Question 5 (See A-1, above)

Note: For confidentiality, respondent identifying information may have been removed.

"As professionals, we instructors constantly stress the practical implications of what our students are learning. We bring field experience into our courses so that students NEVER feel that what we are telling them to learn is simply theory."

"I would like to see better research into tools and/or technologies. For instance, there are more than 30 antivirus products on the market. Which is the best one? What would be the best antivirus strategy? When you think about it, there should be NO antivirus products needed because better work should be done plugging OS vulnerabilities in the first place. We need people who can research the best state-of-the-art techniques that solves EVERYONE's problem."