The Contribution of the CISSP (Certified Information Systems Security Professional) to Higher Education Research

Randy Brown
rwbrown@tamuct.edu
Department of Computer Information Systems
Texas A&M – Central Texas
Killeen, TX 76549

Abstract

Information Security has been a challenge since humans began keeping information. With the advent of computerized data and computer networks, that challenge has increased dramatically. Not only are more breaches occurring, but public knowledge about those breaches is now commonplace adding to virtual hysteria concerning data and information security. To combat the challenge, many organizations are turning to trained and experienced security specialists. Educational institutions are adding curriculum to support the training and education of security professionals. To ensure quality education, many institutions are relying on security certified instructors. One certification highly sought after is the Certified Information Systems Security Professional (CISSP). The educational benefits of CISSP led courses is quite obvious. What is not as obvious is the contribution of the CISSPs to the academic body of knowledge. This paper is an attempt to summarize the current contribution of the CISSP to the academic body of knowledge and open a dialog about the expectations of CISSP to higher educational research.

Keywords: CISSP, Information Security, Security Education, Security Research

1. INTRODUCTION

A Brief Overview of Information Security

There are many parts to Information Security. Cryptography, perhaps the oldest form of Information Security, has been around for a very long time. As early as the 1900s B.C. (and perhaps even earlier), the ancient Egyptians developed hieroglyphics and the ancient Sumerians developed cuneiform. From substitution and transposition ciphers, to modern digital encryption, there have been numerous iterations of cryptography and cryptanalysis. Some of the most notable have occurred in recent history and utilize machinery to improve the capabilities, such as Enigma in World War II (Kahn, 1996).

The modern age of computers and networks further impacted cryptography with digital encryption techniques, ranging from the Data Encryption Standard (DES) in the 1970s to the Advanced Encryption Standard AES in 2001, the Triple DES, and various wireless standards (Stewart, Chapple, & Gibson, 2015). After cryptography, perhaps the oldest issues surrounding Information Security are Physical Security and Social Engineering.

Physical Security deals with preventing others from being able to physically get to the data. We've all heard of buried treasure with secret maps showing "X" marks the spot! That's really not too far off the mark. Physical security includes locked doors (of varying sophistication), fences, guards and guard dogs, cameras, lighting, etc. As technologies advance, so do the capabilities of physical security (Stewart et al., 2015).

Social Engineering is the art of getting someone to divulge information they shouldn't. Some of the best known social engineers are probably Susan Headley and Kevin Mitnick. Susan was active in the 1970s and 80s and is known for hacking into military computers. She would often obtain the information by having sex with military officers, then go through their belongings to find usernames, passwords, etc. while they slept. She was involved in phreaking with Kevin Mitnick, but framed him after they had a falling out, leading to his capture and conviction in 1995. Kevin was a gifted social engineer and hacker in the 1990s, but after his arrest, conviction, and five-year jail term, he is now a widely sought-after security consultant. He is heavily into testing computer security strengths, weaknesses, and loopholes. He also involved in security awareness training and mobile intrusion detection systems (Johnson, 2010).

The Internet has been the greatest facilitator to information security attacks. It enables anyone with a computer to have access to virtually anyone else with a computer, as long as they are connected to the Internet. Even computers that aren't connected to the Internet risk intrusion through dial-up connections or lax physical security. There are loopholes and backdoors into many different computing and networking operating systems, computer applications, smart phone apps, etc (Stewart et al., 2015). While these problems have been around for many years, recent events are really bringing the issues into focus. In the past few months alone, there have been notable security breaches utilizing the Internet. Equifax was breached putting the data of over 145 million people at risk. Yahoo revealed that over 3 billion accounts were hacked. Russia's alleged influence on the last presidential election. Uber had the data of 57 million customers stolen. Ransomware, where hackers lock systems and require payment for unlocking, is on the rise with payments exceeding $2 billion in 2017 (Larson, 2017). There seems to be no end in sight.

The Information Security Professional

To combat the increasing Information Security needs, organizations are turning to Information Security Professionals. Those trained and/or experienced specifically in Information Security. Certifications can help identify experts in various areas of Information Security. Certifications range from entry-level or area specific, such as GIAC Security Essentials and Secure+, to others require more experience or cover wider ranges of topic areas, such as Certified Ethical Hacker (CEH) and Certified Information Security Manager (CISM) (Anderson & Schwager, 2002; Cooper, 2016). One of the most widely recognized and accepted certifications is the overarching Certified Information Systems Security Professional (CISSP) offered by the International Information Systems Security Certification Consortium (ISC)2. The CISSP covers a wide range of security areas or Domains (there are eight), and requires candidates to have five years' experience in at least two of them (Stewart et al., 2015).

Many educational institutions are offering certificates, degrees, concentrations, etc. in Information Security. To make these programs more attractive to students, many institutions are looking for instructors who are certified in at least some area of Information Security (Andersson & Reimers, 2009; Frank & Werner, 2011). As it has the widest coverage of security domains, the CISSP is one of the most sought-after certifications for educators. However, teaching is not the only focus of higher education – increasing the research and body of knowledge is also very important. In addition, "Advance and protect the profession" is one of the prime canons of the CISSP code of ethics (Stewart et al., 2015). So, the focus of this paper is on the contribution of the CISSP to the academic body of knowledge.

There are two parts to this study. The first part is to discover what is being written about CISSPs and the second is to determine what is being written by CISSPs. This two-pronged approach gives a wholistic perspective on how CISSPs are influencing academia and adding (or not) to the body of knowledge. While there is no requirement for non-CISSP authors to write about CISSP topics, the research may still provide insights into the importance of CISSPs to higher education. CISSPs themselves, on the other hand, are expected to contribute to the profession, so how academic CISSPs are adding to the educational body of knowledge may be useful.

2. LITERATURE ANALYSIS

The first step in analyzing the contribution of the CISSP was to find all the academic articles written by or about them. An extensive search of article databases was conducted, searching for the term "CISSP". The included computer-related databases were: ACM Digital Library, IEEE Xplore, Applied Science and Technology Source, ScienceDirect, and ProQuest Central. Disciplines other than computers might also utilize CISSP as authors or topics, so the search also included Academic Search Complete and Business Source Complete. The search yielded 207 articles spanning 1995 to the early 2017, when the

search was conducted. Table 1, below, shows the yearly distribution with one article in 1995 to a high of 26 in 2013. Interestingly, the number of articles each year increased from the one in 1995 until 2007 when the distribution leveled off at about 17 articles per year, with the notable exception of the 26 articles in 2013. The appearance of the conference proceedings and the ISEDJ journal are greatly enhanced by standardized formatting.

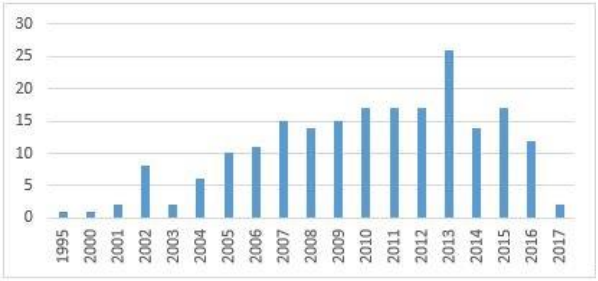

Table 1: CISSP Annual Article Distribution

The 207 articles were published in a wide range of 122 different journals. As expected, many of the journals were computer related, but not necessarily security related. There were, however, several that were not specifically computer related, such as the International Journal of Logistics Management, which was in the top eleven journals by article count – tied for number nine with two others. Table A-1 in the Appendix shows the top eleven journals by article count. *The Journal of Digital Forensics, Security and Law* led the list with 13 articles.

There were 108 articles with at least one author being a CISSP and 109 articles about CISSPs. This total of 217 and reflects that some CISSP authors also wrote about CISSP topics. There were only 19 non-CISSP authors who wrote papers specifically about CISSPs, leaving 80 articles where the CISSP was only mentioned in passing and the CISSP contribution was negligible. These "in passing" articles have been removed from the remaining analysis.

Surprisingly, only about half (59) of the articles written by CISSPs deal specifically with Information Security. Many are on other topics or industries. Table 2 shows the top industries represented by CISSPs as authors. In addition to the top industries, a column for editorials has been included as there were several represented in the articles by CISSPs. All 19 of the non-CISSP authored articles were specifically about Information Security and are not represented in Table 2.

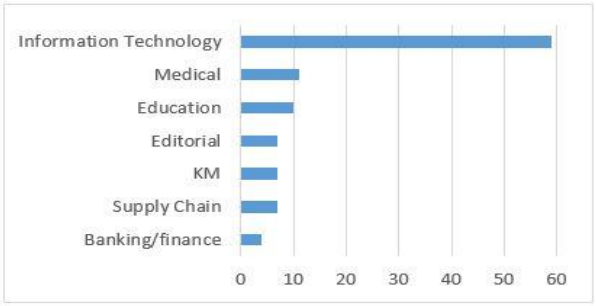

Table 2: Industry Count

There were quite a few different topic areas represented by the articles found. As expected, Information Security was the largest area, with Education and Risk Management the next popular. Table 4 shows the distribution of topics for the combination of CISSP and Non-CISSP Authors. Please note that there is some overlap between topic areas as the focus of a paper may be on Information Security AND Education Security. Also note that ALL articles represented in Table 3 are based off the Security contribution, so there are fewer in Education and Medical than are represented in Table 2, which includes Medical and Education, but not necessarily overlapping with IT Security. For the Non-CISSP authors, the most popular topic area was in Education Security, followed by Interviews.

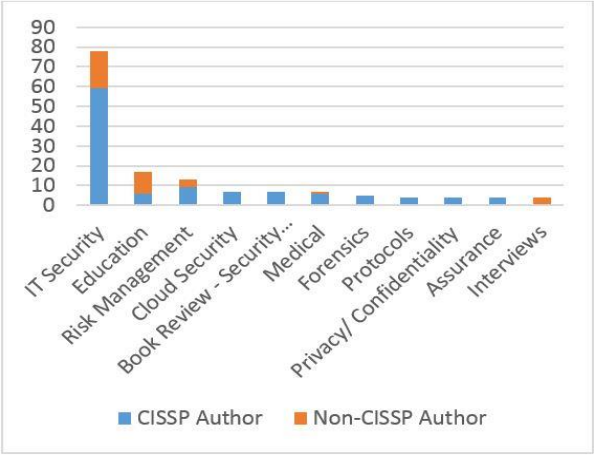

Table 3: Security Topic Count

As seen in the previous charts, CISSPs write about a variety of topics, many of which are not related to Information Security. An analysis of who writes what is needed. The 108 articles by CISSPs were written by only 77 different authors. 65 (84%) of the authors have only a single article with the CISSP certification listed as a credential. 51 (66%) wrote at least one Information Security based article. Table 5 shows the top seven authors based on total number of articles and total number related to Information Security. Of

the top seven, only Author 5 wrote solely on Information Security.

Table 4: Article Count by Author

3. CONCLUSIONS

This study has attempted to quantify various aspects of research about and by CISSPs as represented by the academic body of knowledge. There are two notable limitations to the study. The first is that not all authors with CISSPs include that credential when publishing their work, which will lead to some articles remaining undiscovered. The second limitation is the database selection. The collections used are not all-encompassing and there could be works published by or about CISSPs in other sources.

In spite of the limitations, this study has provided some valuable insight into the contribution of the CISSP in academic research, both from an author perspective and as a topic for research. Two things stood out to the author about the findings of this study. The first is the surprising percentage of CISSPs who are NOT publishing Information Security related studies. It is understood that many academics have multiple areas of interest; however, it was a surprise to find that nearly half 45% (49/108) articles by CISSPs were not specifically security related. On the flip side, with 66% of the CISSP authors writing at least one security related article, the representation is not all bad.

The second notable finding is the flatness of the article by year progression. As information security comes more and more to the forefront and the number of CISSPs in academia increases, it would be expected for articles by and about CISSPs to continue to rise in number. In fact, the opposite seems to be true as the numbers for 2016 show a marked decrease in quantity of CISSP articles. It is hoped that this paper might encourage more discussion and articles about CISSPs in Higher Education.

4. REFERENCES

Anderson, J. E., & Schwager, P. H. (2002). Security in the information systems curriculum: Identification & status of relevant issues. *The Journal of Computer Information Systems, 42*(3), 16-24.

Andersson, D., & Reimers, K. (2009). CIS and Information Technology Certifications: Education Program Trends and Implications. *i-Manager's Journal of Educational Technology, 6*(3), 34-41.

Cooper, M. (2016). Adventures in Ethical Hacking. *ITNOW, 58*(3), 36-37. doi:10.1093/itnow/bww074

Frank, C. E., & Werner, L. (2011). *The value of the CISSP certification for educators and professionals*. Paper presented at the Proceedings of the 2011 Information Security Curriculum Development Conference, Kennesaw, Georgia.

Johnson, L. (2010). COMPUTER CRACKING: The case of Kevin Mitnick. *Forensic Examiner, 19*(3), 22-23.

Kahn, D. (1996). *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*: Scribner.

Larson, S. (2017). The hacks that left us exposed in 2017 from http://money.cnn.com/2017/12/18/technology/biggest-cyberattacks-of-the-year/index.html

Stewart, J. M., Chapple, M., & Gibson, D. (2015). *CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide*: Sybex.

APPENDIX

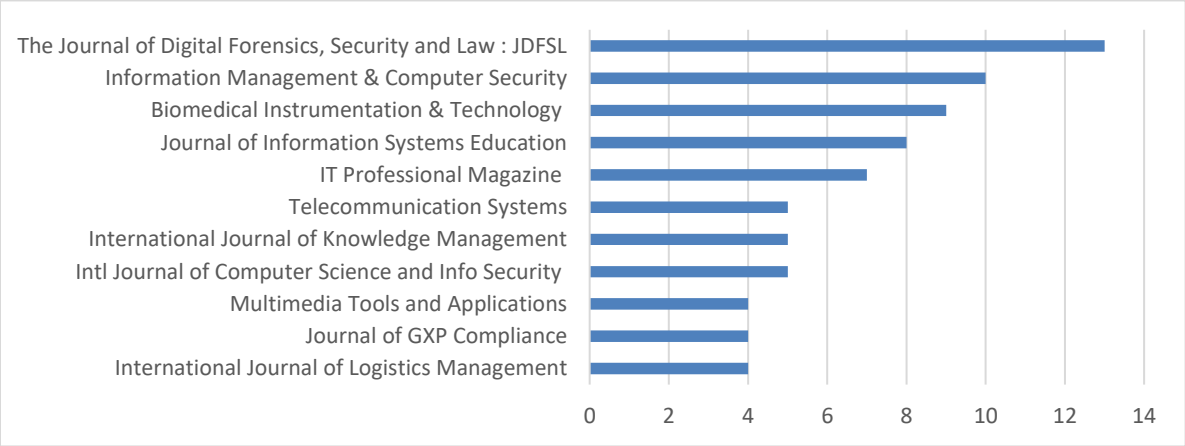

Table A-1: Article Distribution by Publication