Using Cognitive Task Analysis to Investigate the Contribution of Informal Education to Developing Cyber Security Expertise

Michael Champion[1], Shree Jariwala[2], Paul Ward[1], Nancy J. Cooke[3]
[1]University of Greenwich, London, UK
[2]Philips, Seattle, WA, USA
[3]Arizona State University, Phoenix, AZ, USA

Current education systems must respond to meet the increasing need for cyber security and information technology (IT) professionals. However, little research has been conducted on understanding the development of expertise in cyber security and IT, the efficacy of current systems designed to accelerate expertise and/or train cyber security and IT professionals, and the perceived efficacy of these systems rated by the professionals themselves. Moreover, virtually no research exists with respect to the benefit of traditional (classroom-based) formal education compared to informal (self-taught) learning in these complex settings. This paper attempts to address these questions through the use of an online survey of professionals and a follow-up interview with professionals examining this question.

INTRODUCTION

There is an increasing demand for cyber security professionals across industries, organizations, and governments. Recently the U.S. Dept. of Defense called for the increase of cyber security personnel by 4,000 signifying a significant increase over the 900 currently employed personnel (Brannen, 2013). This has been echoed by other governments and in industry. Such a leap in employment requirements is in response to the growing concerns within government agencies about the security of their computer networks. Reports from Verizon (2013), McAfee (2013), and Cisco (2011) are just a few that illustrate the precarious state of Internet and cyber security in general.

In order for any nation to keep up with the rising demand for cyber security professionals we must first understand the developmental and educational trajectory of cyber security professionals. Herein lies a problem. In a report by the U.S. General Accountability Office (GAO) (U.S. Government Accountability Office, 2012), the GAO found inconsistencies between and within agencies about the job requirements listed that comprise a cyber security position. For example, an individual may follow an educational and certification route when training to become a Network Engineer, but that route (and any associated program of study) is unlikely to fully prepare that individual for the actual position. This may be due to any number of factors including limitation of the scope of study, inadequate practical experience, incorrect or incompatible practical experience, and so on.

When we reviewed literature from the human-centric side within the cyber domain, we found little work investigating *what* cyber security professionals were expected to learn, nor *how* they were expected to learn a given task. This is not unsurprising since research on learning in complex domains is limited, and generalization from ‘learning research’ (often conducted in laboratory settings) to complex domains is, at best, difficult (Hoffman, et al., 2014). In brief, we share a growing concern that the human-centric portion of cyber security has insufficient information about the about educational, demographic, and skill-based backgrounds to help inform and educate the future cyber expert.

A number of articles have addressed the issue of education in the cyber domain. However, few researchers have examined the general educational background of practicing cyber security personnel and their developmental trajectory in order to better understand successful educational methods. In this paper, we have investigated two areas of education pursued by most professionals en route to expertise: Formal education and self-taught, informal education. Formal education is any education undertaken that is a structured, classroom or class-like (including online classes), that provides education around any given topic. Informal education is considered to be self-taught and outside of the classroom, even if the nature of the subject originates from the classroom but does not cover the extent to which the student investigates the subject.

More broadly, research in this area has examined the motivational factors of STEM (Science, Technology, Engineering, and Math) students (Shell & Soh, 2013), but has largely focused on formal (rather than informal) education. Other research has investigated alternative practices to applying learned materials in the form of exercises run through universities and academies, such as the International Capture The Flag (iCTF) games by the University of California, Santa Barbara (Childers et al., 2010) and the Cyber Defense Exercises (CDX) by the National Security Agency (Dodge, Ragsdale, & Reynolds, 2003). Although, many more examples of large-scale cyber exercises exist, the research in this area has not examined the developmental, educational, and training-related pathways to success in such events.

The aim of this research was to investigate the pathways followed by cyber security professionals, especially those operating at self-reported intermediate, high and expert levels of skill. This research was conducted in two stages. The first stage was an online survey that the first author conducted while at a University in the Southwest of the United States.

Copyright 2014 Human Factors and Ergonomics Society. DOI 10.1177/1541931214581064

Within this survey a wide range of topics were covered and were largely education focused. The second stage was a more formalized Cognitive Task Analysis conducted at the first author's current university, the University of Greenwich, UK. In this paper we focus specifically on the educational backgrounds of the individuals from this CTA–which, in its full form is ongoing. The guiding research question used to examine both datasets was:

Do cyber security personnel benefit more from formal or informal education?

STUDY 1

Method

Participants. One hundred and ninety-seven responses were collected via an online web survey. Of those, 131 responses were used in the analysis based on self-reported occupation, completeness of data, and outlier analysis. Of these 131, a subset was utilized in each analysis based on the completeness of each section. The specific number of participants is provided for each analysis.

Most respondents were recruited by an email invitation through various listservs and organizations. A smaller portion of respondents were recruited through a professional social networking site.

Materials. The survey consisted of six sections: Background, Education, Expertise, Activities, Tools, and Teamwork. Question responses ranged from dichotomous "yes/no" responses, to Likert-scale and open-ended responses. Aside from initial screening questions, subsequent questions were not required to be answered within the survey. In this study, we focused on specific aspects of the Background, Education, and Expertise sections as follows.

The Background section requested basic demographic information, including whether they were currently, or had been previously, employed within the field of cyber security. To further screen responses, respondents were also asked to report their current job title**.**

The Education section requested information about both formal and informal education, including highest level of attained formal education, years spent in formal and informal education activities, and preferred sources of educational materials.

The Expertise section requested information about self-reported level of expertise in any one of eight sectors of cyber security: Cyber Defense, Cyber Offense, Government, Military, Corporate, Education, Freelance and Personal, and Non-Profit. Participants responded using the following scale: (1) no level of skill, (2) minimal level of skill, (3) intermediate level of skill, (4) high level of skill, (5) expert level of skill. Respondents were also asked to characterize what they felt were requirements of someone at an expert level. The remaining sections of the survey were not utilized within the current analysis.

All materials were provided online and published via a popular online survey service. They were accessible through any internet browser.

Procedures. Participants were invited to participate in the online survey through several stages of advertisements. To aid participation rates, they were given the opportunity to enter a raffle for a $25 gift card to a popular online shopping site.

At the beginning of the survey an explanation of the informed consent procedure was provided, and informed consent was obtained prior to completing or withdrawing from the study. The survey took approximately 20 minutes to complete.

Data analysis. First we explored the frequency data to report the general experience of each self-reported skill group. To examine whether there were differences in the amount of formal and informal education received by each skill level, we conducted two separate one-way ANOVAs with time spent in formal education and time spent in self-taught, informal education as the dependent variable in each analysis. Their highest level of self-reported skill (e.g., in their specialty cyber area/sector) was used as the between-participant factor in each analysis. Because too few participants reported operating in their current specialty area/sector with no skill level (n = 1) or with a minimal level of skill as being their highest attained level (n = 5), only those reporting that they had attained an intermediate (n = 36), high (n = 27) or an expert skill level (n = 25) as their highest level of skill were included in the analysis, unless otherwise stated.

In addition, to examine the breadth of skill attained we conducted a one-way ANOVA on the number of areas in which they self-reported being at an intermediate level of skill or above. Their highest level of self-reported skill (e.g., in their specialty cyber area/sector) was used as the between-participant factor. As per the analysis of formal and informal education, only those reporting that they had attained an intermediate, high or an expert skill level as their highest level of skill were included in the analysis

Results

Background. Individuals who reported having no work experience within the field of cyber security were omitted from the analysis. Reported job titles were categorized and coded for similarity. Before removal of respondents who did not report intermediate or higher levels of expertise, over half (57%) of the 99 participants who responded to this question stated their job title as Information Security Analyst or Manager. Sixteen percent of the participants were System Administrators, 18% were in Senior Management Roles, and 8% were in Research, Teaching, and Academia.

Education and Expertise. Respondents were asked to indicate their highest level of education attempted and to rank their own expertise within a given area. The responses in this question are not independent and only the highest education level the respondents indicated that they attempted were included. Out of the 81 responses to the question about highest attempted education, an equal number of participants attempted undergraduate and graduate level (34.5%, or 28 out of 81). Nineteen (23.5%) respondents indicated that they only engaged in self-taught education. However, when a separate analysis was conducted on the responses not controlling for independence, 85.2% (69 of 81) participants reported engaging in self-taught education. Three participants (3.7%) reported attempting only Associate's College, and 3 (3.7%) reported attempting Post-Doctoral work. Although more formal educational avenues are being made available to analysts, the data suggest they rely heavily on being self-taught; participants reported a high number of years self-taught informal education, averaging 12.62 years (SD = 7.03) compared to years spent in post-high school formal education, averaging 5.31 years (SD = 3.39). Ninety-five percent (89) of the 94 respondents, before removal, who responded to the question about experience were practiced in cyber defense; 19% had 3-5 years, 29% had 6-10 years, and 23% had 11-25 years of experience. Two thirds of the respondents (60 out of 89) reported that their cyber defense skills were at an intermediate level or higher. Education was the industry with the most respondents with experience. (See Table 1.)

In contrast, fewer were practiced in cyber offense. Half of the respondents (40 out of 95) had no experience in cyber offense; 33 had 1-2 years, 15 had 3-5 years, and 17 had over 5 years of experience. However, when respondents rated their own offensive skills, the data were skewed: more respondents reported having no to moderate skills (no skill = 25; minimal skill = 20; moderate skill = 32) than being highly skilled or expert (highly skilled = 8; Expert = 2). This pattern may be indicative of the respondents learning the skills of cyber offense, but only utilizing them within a defensive nature.

When respondents were asked to indicate what feature an individual would need to obtain a high level of skill, or become an expert within their area, respondents overwhelming indicated, "experience" (36 of 91, 40%). This feature was ranked higher than pure knowledge and education (12 of 91, 13%), and performance (12 of 91, 13%). Respondents were then asked to rank sources of information and knowledge from either: books, webpages (non-tutorial), online training, classroom based courses, trial and error (self-exploration), on-the-job training, and "other". Of the 7 categories, on the job-training had the highest mean ranking whereas classroom based education (ranked 5th) was similar in ranking to other forms of education received via books, webpages (non-tutorial), and trial and error (self-exploration). (See Figure 1).

Differences in extent of formal and informal education at each self-reported skill level. A correlation analysis indicated that the time spent in formal and informal education was not correlated (Pearson's r = .023, p = .866), hence, we conducted separate ANOVAs on the years spent in formal and informal education data. For years of formal education, there was no significant effect of highest self-reported skill level, ($F(2,66)$ = 1.072, p = .348). Those with intermediate, high and expert levels of skill did not differ in the amount of formal education accrued. For years of informal education, there was a significant effect ($F(2, 66)$ = 4.689, p = .012). Those that reported their highest level of self-reported skill as being at an intermediate level had less years of informal education (mean = 9.64 years) compared to those self-reporting at a high skill (mean = 14.59 years) and expert skill level (mean = 14.73 years).

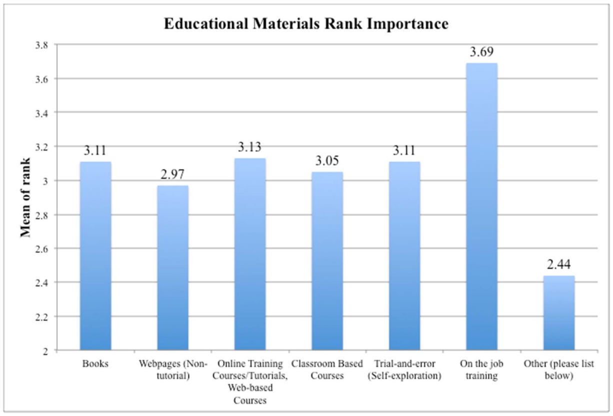

Figure 1. Ranking means of educational material importance.

Breadth of skill attained across areas/sectors. The ANOVA data indicated that experts reported a high number of areas/sectors in which they were currently operating at their highest level of skill level ($F(2, 81)$ =11.434, p = .000). Those who reported their highest level of self-reported skill as being at an intermediate level had operated at that level in 2.88 areas/sectors, compared to those self-reporting at a high skill level (mean = 3.96 areas/sectors) and expert skill level (mean = 5.27 areas/sectors).

Summary

Those self-reporting at a high- and expert-skill level (compared to intermediate) had accrued more experience in self-taught, informal education. All three self-reported skill levels had similar levels of formal education. Of note, self-reported experts had a broader level of expertise than highly skilled individuals who, in turn, had a broader level of skill than those at an intermediate level.

Frequency of Years of Experience within Specific Industry

Industry	None	<1 Year	1-2 Years	3-5 Years	6-10 Years	11-24 Years	25+ Years
Cyber Defense	10	3	9	19	27	22	5
Cyber Offense	40	11	12	15	8	8	1
Government	61	5	9	9	9	0	1
Military	75	1	4	9	2	2	1
Corporate	40	3	12	11	10	12	4
Education	18	4	12	20	21	17	6
Freelance/Personal	49	5	11	13	6	8	2
Non-Profit	57	8	9	6	6	6	1

Table 1. Frequency of years of experience within specific self-reported industry. Respondents were able to select multiple categories to indicate their areas of experience and years of interaction.

STUDY 2

The aim of this study was to use the cognitive task analysis (CTA) method of interviews to explore the nature of the respondents' interaction with the cyber security field. Education, especially self-taught, informal activities, in which highly skilled and expert cyber security professionals had previously engaged, was a central theme within the questioning. Although there is a vast body of literature on the study of expertise more generally, we know very little about the specific types of practice- and training-related activities that help accelerate the development of expertise of individuals working in cyber domains.

Methods

Participants. The responses for the CTA at the time of this writing totaled 15. Due to the nature of the responses, only 10 respondents were utilized in the present analysis. Respondents were recruited via listservs and an online forum website. Each respondent was screened to ensure they were currently, and/or had previously been, employed in a related sector of the cyber security industry before they were included in the study.

Materials. Skype™, text-based chat (Google™ Chat, etc.), or email was used as means to conduct the CTA. This was a semi-structured questionnaire-based interview that allowed the participants to explain and explore their own background within cyber security. The interview started with the respondent's current demographic information, and then proceeded to explore the respondent's initial interactions with computers whether at a professional level or personnel level. The interview then explored the complete educational backgrounds of the respondents for both informal and formal sources. At each chance, responses were probed to remove any ambiguity in a respondent's response.

Procedures. The CTA was conducted through one of three methods of communication, which was pre-selected by the respondent. This process did not offer any compensation for participation. All interviews were recorded either within a text-based log or an audio recording of the Skype™ call.

Respondents completed the informed consent process via email prior to participating in the study. For those selecting a phone call or text-based chat, the next step was the direct interview. For those selecting the email-based interview, they were sent a brief questionnaire to help aid the interviewer in selecting questions to probe, and to reduce the amount of back and forth between the interviewer and interviewee.

The length of the interview varied dependent on the modality of the interview. Vocal/Skype™ based interviews lasted on average 1.5hrs whereas text-based conversations lasted between 4 and 5 hours, spread across several days. For those electing email based communications, the exchanges ranged from only 5 emails before a respondent stopped responding and 40 emails.

Responses were then collected and analyzed through varying methods. The majority of the responses were coded and categorized. Responses resulting in definitive statements and demographics were coded and recorded.

RESULTS

Although the CTA was designed to investigate broader issues, here we present only data from those portions of the CTA relating to the respondents' view on education and how it helped develop their career and knowledge base.

Background. Two respondents reported being employed as an IT Security Analyst. The remaining respondents listed: Freelance Corporate Security Officer, Security Officer, Software Engineer, IT Technical Security, Business Analyst, Researcher, Information Security Architect. One respondent did not provide their current job title.

The average age of the respondent was 32.1 years of age. The gender distribution was highly skewed towards males with 9 males and 1 female. Two respondents had prior military service, one of which had service within a computer-related field. Every respondent reported having, or had, professional certifications with the quantity of certifications per individual ranged from 1 to 10 (mean = 4, n = 7).

Computer Experience. Respondents were asked when they were first introduced to a computer as well as their age when they felt they gained a level of advanced aptitude within computer technology. The average introductory age was reported as 7.1 years old, with the average age of gaining an advanced level of aptitude being 12.9 years of age. In the intervening period (5.8 years), respondents indicated their activities consisted of video game play, learning to type, and learning to use a computer.

Education. Of the 10 respondents, 3 reported having some college but no degree, 2 reported having an Associate's degree only, 2 reported having Bachelor's degrees only, 2 reported having both Bachelor's and Master's Degrees, and 1 had a Doctorate. However, the formal education of four of the respondents (1 at Bachelor's, 2 at Master's, and 1 at Doctorate level) was not related to cyber security or computer science.

Self-education (informal) education was difficult to assess accurately for each individual given the early starting age for many. To account for this, the age at which the respondent expressed an advanced level of aptitude with computers (e.g., surpassing power user skills) use with computers was subtracted from their current age to give a number of years of advanced experience. This ranged from 15 years to 27 years (mean = 18.5 years).

Nearly all respondents explicitly stated that they began their advanced aptitude towards computer science/IT through informal education and experience. When asked about the deciding event that influenced them into the computer world, the majority indicated video games as a major reason (60%, 6 of 10). One of the participants did not indicate a direct catalyst whereas the remaining three participants indicated their direct catalysts were either: Internet growth, Money, or Programming.

Perception of Educational Sources. The CTA explored the self-perceptions of formal and informal education with the respondents. These questions asked if the participant valued their formal education over their informal education or vice versa.

Two respondents equated gaining a degree as a means of "checking the box". That is, the respondents felt that the fact of having a degree was more beneficial than the information they gained within the degree. Two additional respondents did not see the need for even obtaining degrees as they felt the field was far more experience/merit-based.

One respondent stated that the formal education process actually hindered their ability to learn the material. They substantiated this by stating that the majority of classroom learning was paper based, and not relevant to real-world projects. It was perceived that this was not beneficial and detracted from activities that were more helpful. Another respondent shared similar viewpoints, but expressed that while they were able to learn a fair amount of information on their own, they felt they might not have the depth of knowledge within each area. This individual eventually left the degree program and entered into military service for a computer field and found that more educational.

One respondent indicated that both informal and formal education were necessary. They indicated that formal education was structured and provided a good foundation allowing for more informal education to expand on more practically oriented material. Expanding on this, the respondent thought that formal education could provide explanations of useful constructs and the means to obtain more informal education. A view held by this respondent was that formal education was a requirement for cyber security/IT work, a view not shared by other respondents within this CTA.

Summary

In sum, this CTA aimed to investigate the perception and nature of educational backgrounds of cyber security professionals. Informal education appeared to play an influencing role within the development of cyber security skills, usually starting at a younger age with advanced aptitude later manifested into professional skill. Formal education did show to be beneficial to some respondents; however, other respondents indicated that this was merely a requirement of a job description, rather than a necessity for acquisition of skill.

DISCUSSION

Identifying the beneficial sources of education for cyber security professionals is an important precursor to advancing the pedagogy of cyber security, and the acceleration of expertise in this area. The present study set out to determine the source of education for such professionals in an effort to identify effective practices and frameworks. What was found was a field that was diverse in backgrounds and education, and multiple pathways to excellence.

Study 1 indicated that professionals had far more years of self-taught (12.32 years) education than formal education (4.96 years). Study 2 indicated a similar practice showing an average of 18.5 years of advanced self-taught/self-guided education in addition to formal education.

Although the first study was unable to probe individuals into their educational choices, and the answers provided for other questions, the interview was able to collect first-hand knowledge regarding developmental choices. The data suggest that formal education may not be as valued within computer science/cyber security as it may be in other fields such as psychology. This could be due to the breadth of the information available within the field, the ability to practice this field outside of the classroom and even without any other (physical) peer interaction, or the perception of the value/relevance of current formal educational practices.

Respondents in both studies indicated higher levels of informal education. In the first study, this informal education was shown increase with skill level, particularly between intermediate and high levels of skill and correlated with higher amounts of informal education could lead to higher levels of skill. Moreover, the breadth of skills demonstrated at higher levels suggest that the differences in informal education facilitated learning in multiple areas and/or the ability to apply knowledge in one area to another. The second study reiterated that informal education is highly valued, and sometimes thought of as primary to formal education – which is considered secondary or as needed to fill in requirements.

This paper has attempted to lay the groundwork for investigating the link between informal and formal cyber education, a link that should be investigated further. It may be possible to fully identify and introduce the benefits of informal education into formal education, by adding in the experiential growth of informal education into the structure of formal education. In doing so, it may provide a more robust and well-rounded education, and become a primary driver for formal education. This could allow for greater development and achievement from students within this area.

ACKNOWLEDGEMENTS

The first study was supported by the ARO MURI Grant W911NF-09-1-0525, Cliff Wang, and the other MURI partners. The second portion of this study was supported by the University of Greenwich.

REFERENCES

Brannen, K. (2013, January 31). Wanted: Geeks to help fight Pentagon's cyberwar - Kate Brannen. *Politico.com*. Retrieved February 11, 2013, from http://www.politico.com/story/2013/01/wanted-geeks-to-help-fight-pentagons-cyberwar-86946.html

Childers, N., Boe, B., Cavallaro, L., Cavedon, L., Cova, M., Egele, M., & Vigna, G. (2010). Organizing large scale hacking competitions. *Detection of Intrusions and Malware, and Vulnerability Assessment*, 132–152.

Cisco. (2011). *Cisco Visual Networking Index: Forecast and Methodology, 2010-2015* (pp. 1–16). Cisco Systems.

Dodge, R. C., Ragsdale, D. J., & Reynolds, C. (2003). Organization and training of a cyber security team (Vol. 5, pp. 4311–4316). Presented at the Systems, Man and Cybernetics, 2003. IEEE International Conference on, IEEE. doi:10.1109/ICSMC.2003.1245662

Hoffman, R. R., Ward, P., Feltovich, P. J., DiBello, L., Fiore, S. M., Andrews, D., (2014). Accelerated expertise: Training for high proficiency in a complex world. New York, NY: Psychology Press.

McAfee. (2013). *McAfee Labs Threats Report: Third Quarter 2013* (pp. 1–34).

Shell, D. F., & Soh, L.-K. (2013). Profiles of Motivated Self-Regulation in College Computer Science Courses: Differences in Major versus Required Non-Major Courses. *Journal of Science Education and Technology*, *22*(6), 899–913. doi:10.1007/s10956-013-9437-9

U.S. Government Accountability Office. (2012). *Cybersecurity Human Capital*.

Verizon. (2013). *2013 Data Breach Investigations Report*.