Journal of Information Systems Education

Volume 28
Issue 1
November 2017

Learning Outcomes for Cyber Defense Competitions

Amy B. Woszczynski and Andrew Green

Recommended Citation: Woszczynski, A. B. & Green, A. (2017). Learning Outcomes for Cyber Defense Competitions. *Journal of Information Systems Education*, 28(1), pp. 21-42.

Article Link: http://jise.org/Volume28/n1/JISEv28n1p21.html

Initial Submission: 30 November 2016
Accepted: 24 April 2017
Published: 7 November 2017

ISSN: 2574-3872 (Online) 1055-3096 (Print)

Learning Outcomes for Cyber Defense Competitions

Amy B. Woszczynski
Andrew Green
Department of Information Systems
Kennesaw State University
Kennesaw, GA 30144, USA
awoszczy@kennesaw.edu, agreen57@kennesaw.edu

ABSTRACT

Cyber defense competitions (CDCs) simulate a real-world environment where the competitors must protect the information assets of a fictional organization. These competitions are becoming popular at the high school and college levels, as well as in industry and governmental settings. However, there is little research to date on the learning outcomes associated with CDCs or the long-term benefits to the participants as they pursue future educational, employment, or military goals. For this exploratory research project, we surveyed 11 judges and mentors participating in a well-established high school CDC held in the southeastern United States. Then, we developed a set of recommended learning outcomes for CDCs, based on importance of the topic and participant preparedness for future information-security related endeavors. While most previous research has focused on technology issues, we analyzed technological, human, and social topics to develop a comprehensive set of recommendations for future CDCs.

Keywords: Cyber defense competition, Learning goals & outcomes, Cybersecurity, Information assurance & security

1. INTRODUCTION

Students who graduate from information systems (IS), information security/assurance (ISA), and information technology (IT) programs rarely possess all of the required skills and knowledge needed in order to fill an information security role for an employer right away. High schools, technical schools, universities, and training centers have sought to simulate the work environment to prepare participants for future opportunities. Competitions range from industry-sponsored events where university students protect and defend "digital fortresses" to "War Games" for academics (Angelo, 2006) to the nationally recognized Collegiate Cyber Defense Competition (CCDC).

With breaches making the news, like Russia's alleged compromise of a Democrat National Committee (DNC) email server (Lewis, 2016) and North Korea's alleged cyber thefts (Cha, 2016), it is clear that information security threats will continue to increase, remain dynamic, and be difficult to predict in organizations, much like the scenarios simulated in CDCs. Moreover, the market for information security professionals has increased dramatically, with over 200,000 unfilled information security positions in the U.S. alone – and 1 to 1.5 million worldwide by 2019 (Morgan, 2015, 2016), to go along with an unemployment rate of less than 2% (U.S. News & World Report, 2016). Universities who recognize the importance of providing appropriate information security training (Asllani, White, and Ettkin, 2013) will likely attract more students than those who fail to recognize the need for well-trained information security professionals. For academic institutions to retain relevance and appeal to students, they would be wise to implement more real-world training activities, such as CDCs, to prepare our future information security professionals.

Many experts and researchers have noted the importance of graduating qualified, capable students who can help secure critical infrastructures in government. Colesniuc (2013) suggests that securing cyberspace is at least as critical as securing other infrastructures, such as the water systems and electrical grid, while Thales (2010) stresses the importance of securing national infrastructures. Cyberwar has emerged as a recent threat to governmental infrastructures (Cetron et al., 2009), particularly with government legacy infrastructure systems that were designed many years ago. While some sectors, such as the U.S. water system, have a coordinated information sharing program and methods to combat threats (Edwards, 2010), other legacy infrastructures have not instituted organized responses to information security threats. Security considerations – if designed properly at the time – likely need to be revisited; this is particularly true for science and mathematics servers in the U.S. (National Research Council, 2009) which face relentless attempts by unknown adversaries to compromise government-funded and industry-sponsored research and development projects. To protect national security, Asllani, White, and Ettkin (2013) recommend cooperation across government agencies, from local to state to regional to national alliances. The White House agreed, releasing a policy document that promised increased cooperation across borders and an emphasis on protection of critical infrastructure systems, while ensuring basic human rights and compliance with rules and regulations (Crook, 2011). Mulligan and Schneider (2011) go so far as to

call information security a "public good" and recommend adopting policies and implementing controls such as those used in public health. Clearly, information security remains an essential component of national security. CDCs offer opportunities to simulate real-world environments and prepare students for jobs after graduation.

CDCs have grown in popularity in the past decade. Governmental and industry groups, with an increased focus on STEM education, seek to prime the pipeline for talent at a young age, beginning in middle school or earlier. The first high school CDC – IT-Adventures and the IT-Olympics – was held at Iowa State University (Rursch, Luse, and Jacobson, 2010) in an effort to build interest in and capabilities for information security. At the middle and high school levels, the Air Force Association began offering the CyberPatriot program in 2009 with a small group of eight teams participating. By 2015-2016, over 3,000 students participated in the competition (Air Force Association, 2016). Similarly, the US Cyber Challenge attracts about 10,000 potential information security experts – high school students to help fill the pipeline of college information security majors in the future (Acohido, 2010).

At the college level, NYU boasts the oldest competition, holding its first Cyber Security Awareness Week and associated CDCs in 2004; in 2014, the number of participants had grown to 20,000 students (NYU Polytechnic School of Engineering, 2014). The most well-known college competition, the CCDC began as a small regional competition in 2005, with eight teams participating, and moved to the national level in 2006 (White and Dodge, 2006). By 2016, the CCDC showed tremendous growth with more than 180 schools participating (PR Newswire, 2016). Clearly, there is mounting interest in offering information security training at all levels, combined with a strong need for stimulating and maintaining interest in the discipline, from the earliest ages, to meet the increased workforce demands of the future.

While there are general guidelines and some consistency between the levels of competition (middle/high school vs. 2-year/4-year colleges) and across regions, there are no standardized, agreed upon learning outcomes for all CDCs. Thus, student learning outcomes are non-existent or, at the least, fragmented and inconsistent. Adding other government and industry sponsored CDCs, the learning outcomes become even less clear. Without consistent learning outcomes based on educational input and industry expertise, applied in a similar, repeatable manner, it is difficult to determine the relative worth of these competitions, along with the benefits to students and future employers. Therefore, to understand the concepts that should be included, we investigated a large, well-established high school CDC held in the Southeast U.S. We divided topics into three categories: technology, social, and human, as originally defined by Beznosov and Beznosova (2007). We then reviewed previous research in information security education and CDCs. We combined this research with a survey of CDC judges and mentors to develop a set of learning outcomes that can be used by IS, ISA, and IT educators as they design curriculum for their students.

2. LITERATURE REVIEW

Previous studies have reviewed activities associated with CDCs, although over 90% of the identified issues have been associated with technology or technical considerations (Beznosov and Beznosova, 2007). There is no standardized set of learning outcomes associated with CDCs, with some using Certified Information Systems Security Professional (CISSP) standards (Slusky and Partow-Navid, 2012) and others using components of NSA, NHS, ACM, or ABET curriculum guidelines.

To categorize and study important elements of CDCs, Beznosov and Beznosova (2007) defined technological, social, and human issues. Technological issues refer to "all aspects of computer security that involve purely technological solutions" (p. 422). They use cryptography, access control, intrusion detection, information assurance, and malware as examples of technological issues.

Social issues are defined as "those factors that are due to interactions among more than one person in social or formal organizations and within wider social context" (p. 422). Examples include politics, organizations, and economics. Finally, human issues are "related to or concerned with a person, such as phishing or shoulder surfing" (p. 422).

While this categorization provides a solid framework for future studies, Beznosov and Beznosova (2007) readily acknowledge that their list is not all-inclusive; further, they recognize that multiple items overlap among the categories. Our list of important issues is updated, and more comprehensive than the list proposed by Beznosov and Beznosova (2007), although we concede that our list is not exhaustive either and will need to be updated over time. Further, we carefully analyzed the issues and found several hybrid topics; that is, items that overlapped in two or three of the categories, which has implications for how to model the issues when conducting CDCs. While the overlap was noted and diagrammed in the Beznosov and Beznosova (2007) study, their focus was more on the social issues. We focus on our updated and much more comprehensive list, and model the overlap noted. Now we turn to a review of important issues related to technology, social, and human categories.

2.1 Technology

Beznosov and Beznosova (2007) defined technological issues as those with a specific technical component; we further required the explicit use of one or more technology tools for an item to fit in this category. Technology tools used in the CDC may include firewalls, network monitoring, vulnerability scanning, intrusion detection and prevention, log scanning and analysis, vulnerability scanning, and packet analysis; specific tools, such as Wireshark (https://www.wireshark.org), the most widely used network traffic analyzer, may be provided. We considered information security essential technology skills, preventing and responding to attacks, security policies, security education, training and awareness (SETA), and computer monitoring, along with compliance with laws and regulations, as issues associated with technology and CDCs, as described in the following sections.

2.1.1 Information security essential technology skills: Most experts agree that a proper technology background is essential to securing the organization's IT infrastructure. Fulton, Lawrence, and Clouse (2013) suggested a comprehensive set of skills that students need, including familiarity with operating systems, networking, and computer forensics. Knowledge of Linux and Windows (Fulton, Lawrence, and Clouse, 2013), as well as an understanding of cryptography (Beznosov and Beznosova, 2007; CISSP, 2015; Fulton, Lawrence, and Clouse, 2013; Kim and Choi, 2002), malware analysis (Beznosov and Beznosova, 2007), and telecommunications and network security (CISSP, 2015; Fulton, Lawrence, and Clouse, 2013), are important essential technological skills for information security professionals. A good information security professional uses technology to integrate security with the software development cycle and within the overall architecture and design plan (CISSP, 2015; Ghiglieri and Stopczynski, 2016). Further, professionals must consider usability (Beznosov and Beznosova, 2007) when developing tools to prevent, detect, and recover from information security breaches.

2.1.2 Preventing and responding to attacks: Organizations may use multiple tools to prevent attacks, including access control (Beznosov and Beznosova, 2007; CISSP, 2015; Fulton, Lawrence, and Clouse, 2013) and physical security (Cetron et al., 2009; CISSP, 2015). Organizations that implement proper risk management policies and processes may achieve measurable advantages over their competitors (Fulton, Lawrence, and Clouse, 2013). Proper use of technology protects information assets using appropriate information assurance policies and tools (Beznosov and Beznosova, 2007) to implement information security governance and other information assurance policies (CISSP, 2015; Fulton, Lawrence, and Clouse, 2013). Intrusion detection and protection appliances can also be helpful in responding to attacks (Beznosov and Beznosova, 2007).

Technology tools that relate to cyber defense include the ability to respond to attacks on critical infrastructure (Colesniuc, 2013). Once an incident occurs, IT professionals may use computer forensics (Fulton, Lawrence, and Clouse, 2013) to identify attackers and prevent new attacks. Ideally, IT professionals complete appropriate penetration testing and protect devices from harm (Fulton, Lawrence, and Clouse, 2013). At the same time, they must provide network availability 24/7 (US Army, 2011). Additionally, IT professionals have to determine proper responses during an attack while balancing the needs of customers, employees, and other stakeholders.

2.1.3 Security policies; security education, training, and awareness; and computer monitoring: D'Arcy, Hovav, and Galletta (2009) found that three practices tended to prevent improper use of information systems, including user awareness of security policies; security education, training, and awareness (SETA); and system monitoring. Providing real-time information to stakeholders is a key aspect of information assurance. For instance, the U.S. military provides updated information to all parties using an approach of "network-centric warfare" in an effort to avoid the fog of war (Hill, 2003).

Network monitoring to proactively respond to and prevent attacks is also critical. In 2016, 90% of businesses reported experiencing at least one compromise, with small and medium sized businesses becoming targets of choice as large businesses have improved their information security protection (Cernak, 2016). Thales (2013) reports that almost all organizations in the U.K. have experienced a data breach. As former U.S. Director of National Security, Mike McConnell said "the Chinese have penetrated every major corporation of any consequence in the United States and taken information" (Paglieri, 2015). Plainly, there is a clear and present need to secure information in the public and private sectors. Further, there is a need for properly trained information security professionals to assist in securing organizations across the world.

2.2 Social Issues

Beznosov and Beznosova (2007) defined social issues as those related to politics, organizations, and economics. We provide clarity by expanding the definition to include multiple types of groups that are responsible for completing a related activity. Groups may be organizations, governments, professional industry organizations, or peer groups. These groups set standards, follow cultural norms, and use standard industry and/or organizational policies to accomplish outcomes. For this paper, we consider social issues related to organizations, governments, and other groups, as described below.

2.2.1 Organizations: From an organizational perspective, companies set budgets for protecting information assets while evaluating the economics of security (Beznosov and Beznosova, 2007). Understanding the relative cost of security allows IT and information security managers to effectively argue for and acquire the necessary funding to protect their organization. To persuade business managers, information security professionals must remain abreast of current information security topics (Fulton, Lawrence, and Clouse, 2013) and global information security issues (Cetron et al., 2009; Healey, 2011; Kington, 2008). Successful organizations typically have strong, reinforced information security policies (Fulton, Lawrence, and Clouse, 2013), obvious physical security (CISSP, 2015), and clear information security governance standards (CISSP, 2015) to develop plans to secure the interconnected organization (Cetron et al., 2009; CISSP, 2015).

To minimize and prevent attacks, organizations must install and update appropriate security-related tools. A good risk management plan may even lead to competitive advantage (CISSP, 2015; Fulton, Lawrence, and Clouse, 2013). From the social perspective, a clearly defined plan that defines how people, processes, and technology will respond to an attack is essential (Colesniuc, 2013). Incident response plans should go beyond the role of IT and information security to include all organizational departments, such as accounting, communications, and operations.

Culture will partially determine the organization's ethics (Fulton, Lawrence, and Clouse, 2013). Ethics has a technology and human component as well, as discussed in other sections. Organizations may rely on professional guidelines and industry accepted standards of behavior to regulate professional conduct, negligence, and liability (Harris et al.,

2011). As Hannabuss (2000) noted, IT professionals need to understand negligence and liability issues to be effective employees. In addition, employees need to understand organizational policies on privacy (Crook, 2011; Harris et al., 2011). Organizations that state their privacy policies should follow them for all employees, customers, and other stakeholders. SETA programs with regular refresher courses (D'Arcy, Hovav, and Galletta, 2009) will allow employees to understand, engage in, and participate in appropriate standards of behavior.

2.2.2 Governments: Beyond the organization, governments have different concerns, including cyber terrorism, organized crime, and information technology (Cetron et al., 2009). Governments set information security policies based on regulations, guidelines, and the general culture of its citizens. Public policy goals and the prevailing atmosphere combine as governments make difficult decisions about politics and security (Beznosov and Beznosova, 2007).

When an incident occurs, the government follows policies and processes that allow them to respond appropriately to the incident as part of an overall risk management plan (Fulton, Lawrence, and Clouse, 2013). While risk management may allow businesses to achieve advantages over their competitors, governments who do a good job of risk management are more likely to stay in control and keep necessary systems up and running (Thales, 2013). Policies include investigation and compliance (CISSP, 2015) and adherence to laws and regulations (Asllani, White, and Ettkin, 2013; Fulton, Lawrence, and Clouse, 2013), including those regarding privacy (Crook, 2011; Harris et al., 2011) and individual rights.

2.2.3 Other groups: Informal groups may work together to achieve a common goal in a semi-organized, impermanent manner, but may not be part of a larger organization. For instance, hacktivists, including Anonymous, have become an important concern for organizational and government security (Kelly, 2012); Wikileaks is another example. Groups may work together to use social engineering attacks (Beznosov and Beznosova, 2007; Fulton, Lawrence, and Clouse, 2013), such as phishing, to obtain unauthorized access to systems and networks. Unchecked, these groups may wreak havoc on the organization, similar to the embarrassing data breach suffered by Sony (Elkind, 2015), Julian Assange's coordinated Wikileaks attacks (BBC News, 2017), or the thousands of pages of documents released to the press by Edward Snowden (Macaskill and Dance, 2013). These groups pose a clear and present danger, and they are difficult to locate, secure, and prosecute on a global scale.

2.2.4 Compliance with laws and regulations: IS, ISA, and IT professionals must secure their environments while ensuring compliance with local, regional, national, and global laws, including intellectual property rights (Asllani, White, and Ettkin, 2013; Harris et al., 2011) and privacy rights (Crook, 2011; Harris et al., 2011). Proper design of networks and systems, along with ongoing monitoring and education, help protect intellectual property and other rights.

2.3 Human Issues

Beznosov and Beznosova (2007) defined human issues as those related to or concerned with a person, such as phishing or shoulder surfing. We expand that definition, defining human issues as those where a person is explicitly involved in accomplishing the outcome. The next sections describe human issues, including planning for and carrying out an attack, individual morals and ethics, and social responsibility.

2.3.1 Planning for an attack: Information security professionals must plan for attacks before they happen. Business continuity (BC) and disaster recovery planning (DRP) activities (CISSP, 2015) are people-centered. Phishing and shoulder surfing clearly fit under the human issues as described by Beznosov and Beznosova (2007). Security usability (Beznosov and Beznosova, 2007) also fits under the human issues; perfectly designed security systems are ineffective if users do not use them.

2.3.2 Carrying out attacks: While attacks on critical infrastructure are clearly technological in nature (Colesniuc, 2013), humans often carry out the attacks; thus, we classify attacks on critical infrastructure as a hybrid issue – one with technological and human aspects. Hill's (2003) report of the U.S. using trained personnel to email Iraqi generals during the U.S.-Iraq war, to learn more about the enemy and to give them bad information, fits into this category.

2.3.3 Morals, ethics, and social responsibility: Morals, ethics, and social responsibility are human-centered issues that are important when designing information security and assurance. Fulton, Lawrence, and Clouse (2013) found that including ethics and social responsibility (Harris et al., 2011) in the IS curriculum improves educational outcomes. These issues are important human-centered aspects of a well-rounded information security professional and should be modeled in CDCs. Further, information security professionals should be well-versed on human-centered issues related to professional conduct, privacy, intellectual property, cybercrime, impact on humans, freedom of speech, and green computing (Harris et al., 2011), along with privacy (Crook, 2011; Harris et al., 2011) and professional negligence and liability (Hannabuss, 2000). The end user's personal morals may affect how they perceive sanctions or punishments (D'Arcy, Hovav, and Galletta, 2009), and SETA programs should address those human-centered issues as well.

Based on our literature review, we created a table of topics of important components of CDCs. Table 1 shows these topics and their associated categories: technological, social, and/or human. Hybrid items appear in multiple categories, per our discussion. Although we allowed respondents open-ended "Other" topics, no topic appeared more than once, and thus, we did not include them.

Topic	Category*		
	Technological	***Social***	***Human***
Access control	X		
Attacks on critical infrastructure	X		X
Business continuity and disaster recovery planning		X	X
Computer forensics	X		
Cryptography	X		
Current information security topics		X	X
Cyber terrorism		X	
Economics of security		X	
Ethics		X	X
Global information security		X	
Hacktivists		X	
Incident response	X	X	
Information assurance	X		
Information security governance		X	
Information security policies		X	
Information technology security	X		
Intrusion detection	X		
Investigation and compliance		X	
Legal regulations		X	
Linux fundamentals	X		
Malware	X		
Operations security	X	X	
Organized crime and information security		X	
Penetration testing	X		
Phishing			X
Physical (environmental) security	X	X	
Physical access controls	X	X	
Politics and security		X	
Privacy	X	X	X
Professional conduct		X	X
Professional negligence and liability		X	X
Providing network availability (i.e., email, file transfer, chat, phone) during a simulated attack	X		
Risk management		X	
Securing IT intellectual property rights	X	X	
Securing the interconnected organization	X	X	
Security architecture and design	X		
Security education, awareness, and training programs (SETA)	X	X	
Security usability			X
Shoulder surfing			X
Social engineering		X	
Software development security	X		
Telecommunications and network security	X		
Windows fundamentals	X		
TOTALS	23	25	9
% of total*	53.49%	58.14%	20.93%
* Topics may appear in multiple categories, so the totals do not add to 100%. ** 43 topics total			

Table 1. Cyber Defense Topics and Category

As the table shows, we identified potential topics that fall into all three categories. Unlike previous studies, which relied heavily on technology components, we identified 53.49% of the topics as technological, 58.14% as social, and 20.93% as human.

3. METHOD

We distributed a Qualtrics survey via email to judges and mentors who participated in a well-established, annual high school CDC in the Southeast which held its first competition in 2012. Six teams of six students each participated in the event. Mentors with substantial information security

experience interacted with the teams and provided goals, corrections, and constructive feedback on a weekly basis (or more often) in the weeks and months leading up to the competition, as well as during and after the CDC. Teams also received feedback and evaluative comments from the judges during the competition, within defined limits. The competition was completed in one day, which lasts from 8-10 hours in total.

The survey included all of the items identified in Table 1. We first asked the respondents how well the CDC prepared students for each of the identified topics, using a 4-point Likert scale that included the following choices: Not at all prepared, Somewhat prepared, Moderately prepared, and Very well prepared.

We then considered what students would do after the competition. In effect, what is the dependent variable, and why do we care? First, given that the students were voluntarily participating in a CDC, we determined that they were likely to be interested in information security. Since this was a high school competition, many of the students planned to attend university and/or technical school in the future. Some would pursue immediate employment, although most were inexperienced in information security. We asked the judges and/or mentors how important it was for participants to understand the topic if they planned to major in information-security related fields and go to college or technical school, enter the workforce, or pursue a military career. We collected their input using a 4-point Likert scale that included the following choices: Not at all important, Somewhat important, Moderately important, and Very important.

We sent email messages asking potential participants to respond to the survey and then sent periodic reminders. In all, we sent email messages to 49 judges and mentors; of those, 11 participants responded for a 22.44% response rate. Eight participants completed the entire survey, while three participants had some missing data. When respondents did not answer a question, we simply omitted the item and did not include it in the analysis. We also gathered demographic data on the respondents, including role (judge, mentor, or other), age, and gender.

4. RESULTS

Much like the IT workforce in general, the demographic profile of our respondents mirrors the information security field. Our participants were all white males and mostly in their 40s and 50s; none was of Hispanic origin. They had decades of experience in industry as C-level executives, in academia, and in military service. Seven of our respondents served as judges, two served as mentors, and two served as both judge and mentor.

The respondents assessed student preparation on each topic. Table 2 shows the results separated by category: technological, social, and/or human. Some of the questions in these categories had nine respondents, while other questions had ten respondents, with two respondents adding an "Other" option. Since the middle or average response is 2.5 (with ratings of 1, 2, 3, or 4), we divided the topic scores into the following ranges: <2.00 – Very Low; 2.00-2.49 – Low; 2.50-2.99 – Medium; 3.00-3.49 – High; and >=3.50 – Very High.

Given these ranges, the technological average of 2.41 indicates Low student preparation. Only two topics – Linux and Windows fundamentals – received average responses that were in the High range. Similarly, the social average of 2.12 indicates a Low level of student preparedness. Only social engineering, with an average score of 3.0, received a rating in the High range; all other averages were below 3.0. Human averages fell into the Low preparedness range as well, with an average response of 2.47; no topics received a rating above Medium preparation.

Topic	Technological			Social			Human		
	#	*Avg*	*Rating*	*#*	*Avg*	*Rating*	*#*	*Avg*	*Rating*
Access control	10	2.90	Medium						
Attacks - critical infrastructure	10	2.30	Low				10	2.30	Low
BC/DRP				10	1.80	Very low	10	1.80	Very low
Computer forensics	10	1.80	Very low						
Cryptography	10	1.40	Very low						
Current topics				10	2.80	Medium	10	2.80	Medium
Cyber terrorism				10	1.60	Very low			
Economics infosec				9	1.78	Very low			
Ethics				10	2.70	Medium	10	2.70	Medium
Global infosec				10	1.90	Very low			
Hacktivists				10	2.10	Low			
Incident response	10	2.70	Medium	10	2.70	Medium			
Info assurance	10	2.40	Low						
Infosec governance				10	1.80	Very low			
Infosec policies				10	2.10	Low			

IT security	10	2.80	Medium						
Intrusion detection	10	2.40	Low						
Inv. & compliance				10	2.00	Low			
Linux	10	3.10	High						
Legal regulations				10	1.60	Very low			
Malware	10	2.40	Low						
Operations sec.	10	2.40	Low	10	2.40	Low			
Org crime/infosec				10	1.80	Very low			
Penetration testing	10	1.90	Very low						
Phishing							10	2.90	Medium
Physical security	10	2.70	Medium	10	2.70	Medium			
Physical controls	10	2.60	Medium	10	2.60	Medium			
Politics & security				10	2.10	Low			
Privacy	9	2.56	Medium	9	2.56	Medium	9	2.56	Medium
Prof. conduct				10	2.70	Medium	10	2.70	Medium
Prof. negl. & liab.				10	1.70	Very low	10	1.70	Very low
Provide NW avail.	10	2.40	Low						
Risk management				10	1.90	Very low			
Secure IT IP rights	10	1.30	Very low	10	1.30	Very low			
Secure inter. org	10	2.30	Low	10	2.30	Low			
Security arch./des.	10	2.10	Low						
SETA programs	10	2.20	Low	10	2.20	Low			
Security usability							10	2.40	Low
Shoulder surfing							10	2.80	Medium
Social engineering				10	3.00	High			
Software dev. sec,	10	1.90	Very low						
Telecom & network security	10	2.20	Low						
Windows	10	3.20	High						
AVERAGE		2.41	Low		2.12	Low		2.47	Low

Table 2. Cyber Defense Preparation by Topic

Next we asked the respondents how important it is for students to understand each topic if they plan to attend university or technical schools, with the results shown in Table 3. Overall, our respondents indicated that technological, social, and human topics were of Medium importance for students who planned to pursue further education. Incident response, Linux fundamentals, providing network availability, and Windows fundamentals received ratings of High importance, while computer forensics, cryptography, malware, and securing IT intellectual property rights received Low ratings.

For social topics, ethics, incident response, professional conduct, risk management, and social engineering were rated as being of High importance, while current information security topics, cyberterrorism, economics of security, hacktivists, information security governance, legal regulations, organized crime and information security, politics and security, and securing IT intellectual property rights were rated as Low importance. Finally, for human topics, ethics and professional conduct received ratings of High importance, while current information security topics evaluated as Low importance.

Topic	Technological			Social			Human		
	#	Avg	Rating	#	Avg	Rating	#	Avg	Rating
Access control	8	2.88	Medium						
Attacks - critical infrastructure	8	2.50	Medium				8	2.50	Medium
BC/DRP				8	2.50	Medium	8	2.50	Medium
Computer forensics	8	2.00	Low						
Cryptography	8	2.00	Low						
Current topics				8	2.38	Low	8	2.38	Low
Cyber terrorism				7	2.14	Low			
Economics infosec				8	2.13	Low			
Ethics				8	3.00	High	8	3.00	High
Global infosec				8	2.50	Medium			
Hacktivists				8	2.13	Low			
Incident response	7	3.00	High	7	3.00	High			
Info assurance	8	2.88	Medium						
Infosec governance				8	2.38	Low			
Infosec policies				8	2.63	Medium			
IT security	8	2.75	Medium						
Intrusion detection	8	2.88	Medium						
Inv. & compliance				8	2.50	Medium			
Linux	8	3.00	High						
Legal regulations				8	2.13	Low			
Malware	8	2.13	Low						
Operations sec.	8	2.75	Medium	8	2.75	Medium			
Org crime/infosec				8	2.00	Low			
Penetration testing	8	2.88	Medium						
Phishing							8	2.50	Medium
Physical security	8	2.63	Medium	8	2.63	Medium			
Physical controls	8	2.50	Medium	8	2.50	Medium			
Politics & security				8	2.38	Low			
Privacy	8	2.75	Medium	8	2.75	Medium	8	2.75	Medium
Prof. conduct				8	3.25	High	8	3.25	High
Prof. negl. & liab.				7	2.71	Medium	7	2.71	Medium
Provide NW avail.	7	3.00	High						
Risk management				7	3.14	High			
Secure IT IP rights	7	2.14	Low	7	2.14	Low			
Secure inter. org	7	2.86	Medium	7	2.86	Medium			
Security arch./des.	7	2.86	Medium						
SETA programs	7	2.86	Medium	7	2.86	Medium			
Security usability							7	2.71	Medium
Shoulder surfing							7	2.57	Medium
Social engineering				7	3.14	High			
Software dev. sec.	7	2.71	Medium						

Telecom & network security	7	2.86	Medium						
Windows	7	3.57	Very high						
AVERAGE		2.71	Medium		2.58	Medium		2.69	Medium

Table 3. Importance of Topic for University/Tech School

Next we asked our respondents how important it is for students to understand each topic if they plan to pursue employment in information security or related fields. As shown in Table 4, our participants believe that all three categories – technological, social, and human – are of High importance for those students who plan to pursue employment, with average scores from 3.13 to 3.36. None of the topics had a rating below Medium importance, with the vast majority of topics rated as being of High or Very High importance.

Topic	**Technological**			**Social**			**Human**		
	#	*Avg*	*Rating*	*#*	*Avg*	*Rating*	*#*	*Avg*	*Rating*
Access control	8	3.50	Very high						
Attacks - critical infrastructure	8	3.38	High				8	3.38	High
BC/DRP				8	3.25	High	8	3.25	High
Computer forensics	8	2.75	Medium						
Cryptography	8	2.63	Medium						
Current topics				8	3.25	High	8	3.25	High
Cyber terrorism				8	2.50	Medium			
Economics infosec				8	2.88	Medium			
Ethics				8	3.50	Very high	8	3.50	Very high
Global infosec				8	2.75	Medium			
Hacktivists				8	2.50	Medium			
Incident response	8	3.50	Very high	8	3.50	Very high			
Info assurance	8	3.50	Very high						
Infosec governance				8	2.88	Medium			
Infosec policies				8	3.50	Very high			
IT security	8	3.75	Very high						
Intrusion detection	7	3.43	High						
Inv. & compliance				7	2.86	Medium			
Linux	7	3.71	Very high						
Legal regulations				7	2.71	Medium			
Malware	7	2.86	Medium						
Operations sec.	7	3.29	High	7	3.29	High			
Org crime/infosec				7	2.57	Medium			
Penetration testing	7	3.14	High						
Phishing							8	3.63	Very high
Physical security	8	3.38	High	8	3.38	High			
Physical controls	8	3.38	High						
Politics & security				8	2.75	Medium			
Privacy	8	3.38	High	8	3.38	High	8	3.38	High
Prof. conduct				8	3.63	Very high	8	3.63	Very high
Prof. negl. & liab.				8	3.25	High	8	3.25	High
Provide NW avail.	8	3.38	High						

Risk management				8	3.38	High			
Secure IT IP rights	8	2.75	Medium	8	2.75	Medium			
Secure inter. org	8	3.38	High	8	3.38	High			
Security arch./des.	8	3.13	High						
SETA programs	8	3.38	High	8	3.38	High			
Security usability							8	3.00	High
Shoulder surfing							8	3.38	High
Social engineering				8	3.75	Very high			
Software dev. sec.	8	3.38	High						
Telecom & network security	8	3.25	High						
Windows	8	3.63	Very high						
AVERAGE		3.30	High		3.13	High		3.36	High

Table 4. Importance of Topic for Employment

Next we asked respondents how important it is for students to understand each topic if they plan to join the military. Our respondents indicated that all three categories of topics were of Medium importance for students who planned to pursue a career in military service, as shown in Table 5. None of the topics received ratings of Very High, with several receiving Low ratings.

Topic	**Technological**			**Social**			**Human**		
	#	*Avg*	*Rating*	*#*	*Avg*	*Rating*	*#*	*Avg*	*Rating*
Access control	8	2.88	Medium						
Attacks - critical infrastructure	8	2.75	Medium				8	2.75	Medium
BC/DRP				8	2.88	Medium	8	2.88	Medium
Computer forensics	8	2.50	Medium						
Cryptography	8	2.88	Medium						
Current topics				8	2.38	Low	8	2.38	Low
Cyber terrorism				8	2.75	Medium			
Economics infosec				8	2.25	Low			
Ethics				8	3.00	High	8	3.00	High
Global infosec				8	2.88	Medium			
Hacktivists				8	2.50	Medium			
Incident response	8	3.25	High	8	3.25	High			
Info assurance	8	3.13	High						
Infosec governance				8	2.88	Medium			
Infosec policies				8	3.00	High			
IT security	8	3.00	High						
Intrusion detection	8	3.13	HIGH						
Inv. & compliance				8	2.75	Medium			
Linux	8	2.75	Medium						
Legal regulations				8	2.63	Medium			
Malware	8	2.63	Medium						
Operations sec.	8	3.13	High	8	3.13	High			
Org crime/infosec				8	2.63	Medium			

Penetration testing	8	2.63	Medium						
Phishing							8	3.13	High
Physical security	8	3.25	High	8	3.25	High			
Physical controls	8	3.25	High	8	3.25	High			
Politics & security				8	2.63	Medium			
Privacy	8	2.63	Medium	8	2.63	Medium	8	2.63	Medium
Prof. conduct				8	3.25	High	8	3.25	High
Prof. negl. & liab.				8	2.75	Medium	8	2.75	Medium
Provide NW avail.	8	3.13	High						
Risk management				8	2.75	Medium			
Secure IT IP rights	8	2.25	Low	8	2.25	Low			
Secure inter. org	8	2.88	Medium	8	2.88	Medium			
Security arch./des.	8	2.75	Medium						
SETA programs	8	2.75	Medium	8	2.75	Medium			
Security usability							8	2.63	Medium
Shoulder surfing							8	2.88	Medium
Social engineering				7	2.86	Medium			
Software dev. sec.	8	2.25	Low						
Telecom & network security	8	2.63	Medium						
Windows	8	3.00	High						
AVERAGE		2.84	Medium		2.80	Medium		2.83	Medium

Table 5. Importance of Topic for Military

5. DISCUSSION

CDCs provide an important experiential learning opportunity for students at the high school, university, and post-university levels. While these competitions have become more widespread, there is little consistency in the format of the competition, the topics covered, or the relevance of the competition for the career plans of the participant. In this exploratory study, we used previous research to identify and categorize cyber defense topics as technological, social, or human. Several topics were hybrid, or characteristic of more than one category.

Our survey respondents were Mentors and/or Coaches who participated in a high school CDC. They indicated that the CDC provided students with a generally Low level of preparation across all categories: technological, social, and human, with an overall 2.27/4.00 average, as shown in Table 6. On the positive side, almost all respondents noted that the CDC preparation and competition prepared participants well for Linux, social engineering, and Windows fundamentals, with ratings of 3.10, 3.00, and 3.20, respectively. Clearly, those skills are necessary to build a strong foundation in information security; however, no other skill was rated as High or Very High (3.0 or higher). Surprisingly, our respondents did not believe that the competition prepared students well for several core technological topics, including: attacks on critical infrastructure, computer forensics, cryptography, information assurance, intrusion detection, malware, operations security, penetration testing, providing network availability, security architecture and design, SETA programs, software development security, and telecommunications and network security. All of these categories received overall preparation levels of Low or Very Low. Since the competition asks students to keep a network up and running for routine requests while battling threats, we expected that the participants would have a High or Very high level of preparation for providing network availability and intrusion detection, as well as an ability to respond to attacks on critical infrastructure. Perhaps clearly specified learning outcomes for CDCs would provide a more consistent set of results and better prepare our students for the future. Alternatively, adding competitive aspects to the ISA program, as suggested by Serapiglia (2016), may better prepare students for the aggressive aspects of the CDC.

For social topics, besides social engineering, our respondents rated the competition as Low or Very Low in preparing students for BC/DRP, cyberterrorism, economics of security, global information security, hacktivists, information security governance, information security policies, investigation and compliance, legal regulations, operations security, organized crime and information security, politics and security, professional negligence and liability, risk management, securing IT intellectual property rights, securing the interconnected organization, and SETAs. Perhaps students divide the workload and only one student acquires the social skills needed. Perhaps mentors and/or coaches are more technically oriented. Ensuring equal participation and cross training for team members may improve student preparation.

Topic	CDC	Univ/Tech	Employment	Military
	Preparation	*Importance*	*Importance*	*Importance*
Access control	2.90	2.88	3.50	2.88
Attacks - critical infrastructure	2.30	2.50	3.38	2.75
BC/DRP	1.80	2.50	3.25	2.88
Computer forensics	1.80	2.00	2.75	2.50
Cryptography	1.40	2.00	2.63	2.88
Current topics	2.80	2.38	3.25	2.38
Cyber terrorism	1.60	2.14	2.50	2.75
Economics infosec	1.78	2.13	2.88	2.25
Ethics	2.70	3.00	3.50	3.00
Global infosec	1.90	2.50	2.75	2.88
Hacktivists	2.10	2.13	2.50	2.50
Incident response	2.70	3.00	3.50	3.25
Info assurance	2.40	2.88	3.50	3.13
Infosec governance	1.80	2.38	2.88	2.88
Infosec policies	2.10	2.63	3.50	3.00
IT security	2.80	2.75	3.75	3.00
Intrusion detection	2.40	2.88	3.43	3.13
Inv. & compliance	2.00	2.50	2.86	2.75
Linux	3.10	3.00	3.71	2.75
Legal regulations	1.60	2.13	2.71	2.63
Malware	2.40	2.13	2.86	2.63
Operations sec.	2.40	2.75	3.29	3.13
Org crime/infosec	1.80	2.00	2.57	2.63
Penetration testing	1.90	2.88	3.14	2.63
Phishing	2.50	2.50	3.63	3.25
Physical security	2.70	2.63	3.38	3.25
Physical controls	2.60	2.50	3.38	2.63
Politics & security	2.10	2.38	2.75	2.63
Privacy	2.56	2.75	3.38	3.25
Prof. conduct	2.70	2.38	3.63	2.75
Prof. negl. & liab.	1.70	2.71	3.25	3.13
Provide NW avail.	2.40	3.00	3.38	2.75
Risk management	1.90	3.14	3.38	2.25
Secure IT IP rights	1.70	2.14	2.75	2.88
Secure inter. org	2.30	2.86	3.38	2.88
Security arch./des.	2.10	2.86	3.13	2.75
SETA programs	2.20	2.86	3.38	2.75
Security usability	2.40	2.71	3.00	2.88
Shoulder surfing	2.80	2.57	3.75	2.86
Social engineering	3.00	3.14	3.38	2.86

Software dev. sec,	1.90	2.71	3.38	2.25
Telecom & network security	2.20	2.86	3.25	2.63
Windows	3.20	3.57	3.63	3.00
AVERAGE	2.27	2.61	3.20	2.81
	Key: <2 = Very Low; 2.0-2.49 = Low; 2.5-2.99 = Medium; 3.0-3.49 = High; > =3.5 = Very High			

Table 6. Match Between Level of Student Preparation and Importance of Topic

In the human categories, our respondents indicated Low or Very Low student preparation for attacks on critical infrastructure, BC/DRP, professional negligence and liability, and security usability. Better education on proper security policies and processes could improve these levels of preparation. Further, clearly defined learning outcomes that outline and assess student capabilities may improve scores in these areas.

We investigated further to see how the skills acquired in the CDC experiential learning opportunity matched with pursuit of university/technical education, employment, or military careers. Overall importance of all of the topics averaged 2.61, 3.20, and 2.81 for the categories, respectively. These results were as expected. While some knowledge of the information security topics is important for students who choose to go to university or join the military, much higher levels of overall information security knowledge would be needed for those who seek ISA employment.

Several skills were important across all future opportunities. Windows fundamentals rated as High or Very High for future endeavors, and our respondents believed that the participants were well prepared in this area. Clearly, the way that participants are prepared to use Windows in the CDC is effective, and this is a skill that they are likely to use in the future. Meanwhile, ethics and incident response were rated as being of High or Very High importance while students had a Medium level of preparation.

Providing network availability was rated as Medium or higher importance for all three future opportunities, although students had a Low level of preparation. Since most CDCs simulate attacks on networks, this topic is obviously important. Perhaps coaches and/or mentors should ensure that they focus more on acquiring this skill. Multiple opportunities to ensure network availability in realistic adversarial situations – prior to the competition – may prepare students for this essential skill. Moving toward the use of more hands-on, real-world simulated scenarios in the classroom, and during CDC preparation, may also help.

Risk management was also rated as Medium or higher importance across categories, but students had a Very Low level of preparation. Risk management is policy driven, and thus a social topic. Perhaps requiring detailed risk assessment plans from the teams participating in the CDC would help to alleviate this issue.

Several topics rated as being of High or Very High importance for both employment and the military, but not for those pursuing future educational opportunities. Professional negligence and liability was rated as being of High importance for both, with Very Low levels of student preparation. Information assurance, information security policies, and operations security were rated as being of High or Very High importance for employment and the military, coupled with overall Low levels of student preparation. IT security, phishing, physical security, and privacy were rated as High or Very High importance, while students had Medium levels of preparation. These areas of mismatch between preparation and importance cross all categories – technological, human, and social – and indicate areas where additional efforts should be made to educate students.

CDC participants were rated as being Highly prepared for protecting Linux systems. Respondents indicated that Linux has High or Very High levels of importance for those pursuing future education and employment opportunities and a Medium level of importance for those choosing military careers. From these results, it appears students are well prepared to use Linux in their future endeavors. Educators should continue these efforts going forward.

Numerous topics were rated to be of Low importance for those choosing to pursue future educational opportunities. The topics included: computer forensics, cryptography, current topics in ISA, cyber terrorism, economics of information security, hacktivists, information security governance, legal regulations, malware, organized crime and information security, politics and security, professional conduct, and securing IT intellectual property rights. Interestingly, students were deemed to have Low or Very Low levels of preparation for all of these topics, except current topics in IS and professional conduct, which had Medium levels of student preparation. In these areas and for students pursuing future educational opportunities, there is a good match between the student preparation levels and the importance of the topics.

When looking at the importance of topics for those pursuing future ISA-related employment, our respondents evaluated every single topic as being of Medium or higher levels of importance. It is unfeasible for a single student experiential learning opportunity, no matter how thorough or how well planned, to do a very good job of preparing students for future employment opportunities in all of these topics. Considering that the students in this study were at the high school level, it is even more difficult to train them to be ready to enter the workforce upon completion of the CDC.

Finally, when looking at pursuing military opportunities, all of the topics were rated at being of at least Medium importance, with the exception of economics of information security, risk management, and software development information security, all of which had Very Low levels of importance combined with Very Low levels of student preparation. In these cases, at least, the level of student preparation matches the importance of the topic for future military opportunities, which is a desirable outcome.

Based on our results, we suggest that educators and organizers design CDCs that will meet the following learning outcomes, if many of the participants will be pursuing

university or technical school in the future. At the end of the CDC, participants should be able to:

- Write Linux and Windows scripts to support proper security protocols
- Ensure network availability during a simulated attack
- Develop appropriate incident response plans
- Demonstrate how to overcome typical ethical challenges while maintaining network security
- Properly manage risk using accepted information security policies and procedures
- Respond to social engineering attacks using appropriate security management techniques

For students pursuing information security employment after the CDC, all of the topics were rated at Medium levels of importance or higher. Educators and organizers should consider offering longer and more in-depth study of multiple topics if the intent is to develop professionals who are ready to go into the workforce. If many participants will be pursuing employment opportunities after the CDC, we suggest that educators and organizers design CDCs that will meet relevant learning outcomes. At the end of the CDC, participants should be able to:

- Write Linux and Windows scripts to support proper security protocols
- Provide network availability during a simulated attack
- Demonstrate how to overcome typical ethical challenges while maintaining telecommunications and network security
- Exhibit professional conduct as an IT professional
- Properly manage risk using accepted information security policies and procedures
- Detect and respond to unauthorized network access
- Implement controls to prevent unauthorized access to information assets
- Use physical (environmental) security protocols to protect information assets
- Create and manage incident response plans
- Develop policies and procedures to manage information assurance and ensure operations security
- Create access control procedures to minimize risk
- Respond to attacks on critical infrastructure using information response plans
- Create business continuity and disaster response plans
- Secure the organization against social engineering attacks
- Minimize professional negligence and liability through the use of proper information assurance plans
- Ensure security usability
- Design secure organizational infrastructure plans
- Exhibit understanding of current topics in IT
- Implement IT security policies throughout the software development lifecycle
- Secure the information assets of the interconnected organization
- Ensure privacy of data
- Participate and advise the organization on SETA

As expected, technical topics have a prominent role in preparation for a military career. If many of the participants will be pursuing military careers after the CDC, we suggest that educators design CDCs that will meet specific learning outcomes. At the end of the CDC, participants should be able to:

- Write Windows scripts to support proper security protocols
- Use physical (environmental) security protocols to protect information assets
- Detect and respond to unauthorized network access
- Demonstrate how to overcome typical ethical challenges while maintaining network security
- Create and use incident response plans
- Minimize professional negligence and liability through the use of proper information assurance plans
- Develop policies and procedures to manage information assurance and ensure operations security
- Manage a phishing attack using information security detection and response policies
- Ensure privacy of data

Several learning outcomes are important, regardless of whether students are pursuing education, employment, or military opportunities. Therefore, at a minimum, IS, ISA, and IT educators should model these overarching learning outcomes in all CDCs. At the end of the CDC competition, participants should be able to:

- Write Linux and Windows scripts to support proper security protocols (Technological)
- Implement controls to prevent unauthorized access to information assets (Technological)
- Create and use incident response plans (Technological & Social)
- Use physical (environmental) security protocols to protect information assets (Technological & Social)
- Minimize professional negligence and liability through the use of proper information assurance plans (Technological, Social, & Human)
- Develop policies and procedures to manage information assurance and ensure operations security (Technological & Social)
- Demonstrate how to overcome typical ethical challenges while maintaining network security (Social & Human)
- Respond to social engineering attacks using appropriate security management techniques (Technological, Social, & Human)
- Ensure privacy of data (Technological, Social, & Human)
- Properly manage risk using accepted information security policies and procedures (Social)

The recommended learning outcomes include a mix of technological, social, and human categories, providing balanced exposure for students.

6. CONCLUSION

Our results contribute to IS, ISA, and IT education in several ways. First, we developed an extensive list of topics to consider when developing CDCs. Unlike most previous studies, which have focused almost exclusively on technological areas, we included topics in social and human categories as well. Further, we carefully discussed each topic, noting the hybrid nature of some of the areas of study; that is, some topics fell into more than one category.

We asked our mentors how prepared students were for each of the topic areas after completing the CDC. Then we asked the mentors which topics were most important for students who wanted to pursue or continue their education in information-security related fields, seek employment in ISA, or join the military. We highlighted topics that were important for future educational opportunities in information security, future information security employment opportunities, or military opportunities and then compared to the preparation level of the students after the competition. From that, we developed a set of minimum learning outcomes that educators should consider when seeking to prepare students for future opportunities. While technological skills, such as Windows and Linux fundamentals, were important across all future opportunities, we did find a few surprises. Ethics received a prominent role, as did professional negligence and liability, areas that are more social and human in nature. Another surprising result was the mismatch between the High necessity of providing network availability, with the Low preparation of the students. Since the overall goal of most CDCs is to keep a network up and running during a simulated attack, we anticipated that students would have a High to Very High level of preparedness with that topic; we were wrong. Educators need to make sure that all students receive broad exposure to the basics of keeping the network available and running when under attack.

Our respondents identified only seven topics that were of High or Very High importance for students who wish to pursue educational opportunities, while they identified about a dozen High or Very High importance topics for military service, and about 30 topics that were of High or Very High importance for those who planned to pursue employment. Since we only included 43 topics total, the number of topics for Employment was substantial. Not surprisingly, students need to acquire many skills and capabilities prior to being able to contribute in an information security employment setting. Most CDCs will not prepare students for immediate employment. However, IS, ISA, and IT educators can seek to highlight those capabilities most valued by employees when holding competitions for university students who may soon seek employment. An interesting option is to investigate the learning outcomes of professional/industry CDCs and how they differ from high school or university CDCs. Gabberty (2013) noted positive outcomes from experiential, real-world training opportunities, and designers of future CDCs should carefully consider which topics to cover during simulated attacks. Students may use these experiential learning opportunities and acquired skills to make their resumes more attractive to employers. When hosting CDCs for industry professionals, the competitions may need to be more substantial, cover more topics, and last for a longer time, so that participants get an opportunity to showcase and improve the skills needed for information security professionals.

7. LIMITATIONS AND FUTURE RESEARCH

7.1 Limitations

We delivered our survey online using Qualtrics. Respondents self-selected to participate, and thus the sample is non-probabilistic and may not represent the population as a whole. However, our sample of all white males corresponds to the predominant race and gender qualities seen in information security. Clearly, collection of a more diverse sample, including a representative mix of women, non-white races, and ethnicities of Latino descent, may yield more valuable data.

Further, we had a sample of 11 respondents, which is small, and which may lower the external generalizability of the results. However, the number of judges and mentors for the CDC totaled only 49; thus, our response rate of just over 22% is within an acceptable range. Future studies could enlist the participation of more judges and mentors to validate the learning outcomes we developed. In addition, a 360-degree sample, to include students, peers, industry participants, mentors, and judges, may yield more enlightening information.

In addition, our respondents were judges and mentors participating in a high-school level CDC. While the judges and mentors in our study had significant, decades-long experience as C-level executives, in academia and in the military, a larger, more diverse sample might yield richer results.

Further, while we relied on Beznosov and Besnosova's (2007) original definitions of technological, social, and human issues, there may be opportunities to re-analyze the definitions. There is significant crossover of human and social issues, for instance, and it might be more helpful to analyze two categories (Technological and Social/Human) for simplicity.

Moreover, in some cases, questions could have been clearer. For instance, we asked how important it is for students to understand each topic if they plan to pursue future education without specifying the pursuit of ISA-related degrees. The judges and mentors had information-security backgrounds and would know and understand the qualities needed to be successful in ISA-related fields after the competition. We believe the judges and mentors, whose expertise lies in ISA, focused on information-security related education as we intended. Similar question re-examination may be appropriate for the military question as well. The preparation for future employment specifically asks about information security-related fields as we intended.

We distributed the survey after the CDC ended. Our intent was to gather student preparation levels after the competition, including any preparation done before the competition, along with whatever the student learned during the preparation for the CDC. It is possible some respondents could have misunderstood the question, not knowing if the levels of preparation referred to before or after the CDC; we encourage future researchers to continue to validate and refine our initial scale.

Different types of competitions – university, military, and industry – may require unequal levels of preparation across the topics studied. However, the average rating of the need for a particular topic to be prepared for university/technical school, the military, or employment should be similar, no matter the level of the competition. Particularly when considering the preparation for future employment, high school students are unlikely to be prepared for an ISA position upon completion of the CDC; competitions held at universities and/or with business or government sponsors may see very different levels of preparation for the future than our high school students, particularly regarding preparation for employment.

A focus on the high school level could explain some of the differences in the mean level of preparation as compared to the need for a topic, as shown in Table 6. Gathering data from participants in multiple types of competitions may assist in the development of learning outcomes that are more specific to the future opportunities anticipated, with a focus on matching the importance of the topic for the future opportunity with the students' levels of preparedness. We encourage additional research to evaluate these exciting and valuable experiential learning opportunities.

While we developed learning outcomes based on topic importance and levels of preparation, we did not develop an assessment instrument. Assessment is necessary to determine if participants accomplish the topic areas identified and is needed for accreditation activities if the CDC is part of classroom learning. Future research should validate and assess mastery of the learning outcomes suggested.

Finally, while this paper looked in-depth at learning outcomes for the CDC, event planning and technology setup were beyond the scope of the study. Other authors (Carlin, Manson, and Zhu, 2010) provide excellent advice on the planning side.

7.2 Future Research

The recent Sony and DNC compromises highlighted the need for information security protections for governments and private industry. In some cases, it is important for policy makers to know who is responsible for an attack in order to determine how to respond (Healey, 2011). Knowing how to respond to an information security breach goes beyond simply understanding the technical underpinnings of the attack. An interdisciplinary response, in combination with communications, public relations, marketing, advertising, finance, and accounting organizational units, presents opportunities for those who design CDCs. We should investigate this cross-disciplinary approach to crisis management in the future. What sort of cyber defense simulations should those outside of IS-related majors undergo to prepare them to respond to a crisis? Would a "Cyber League," which allows teams to compete head-to-head (Manson and Carlin, 2010), simulating the popular gaming environment, provide a better learning experience than the short, intense (and not head-to-head) CDCs that are most common? Current CDCs appeal to those interested in IS, ISA, and IT, but we may be underserving other disciplines by not helping them design appropriate crisis simulations and prepare a response. Crisis preparation and response has become an almost routine activity, but a cross-disciplinary approach is necessary to maintain goodwill and to keep customers. CDCs may provide information security students with initial skills, but we must reach across the aisle and capitalize on the expertise of functional areas beyond IT, to make a reasoned, well thought out, and understandable public statement.

8. REFERENCES

Acohido, B. (2010). Wanted: Young Cyberexperts to Defend Internet. Gannett News Service, June 20, 2010.

Angelo, J. M. (2006). Making a Game of IT Security. *University Business*, 9(7), 15.

Air Force Association (2016). CyberPatriot: The National Youth Cyber Education Program (History). http://www.uscyberpatriot.org/about/history.

Asllani, A., White, C. S., & Ettkin, L. (2013). Viewing Cybersecurity as a Public Good: The Role of Governments, Businesses, and Individuals. *Journal of Legal, Ethical and Regulatory Issues*, 16(1), 7-14.

BBC News. (2017). Julian Assange: Campaigner or Attention-Seeker? http://www.bbc.com/news/world-11047811.

Beznosov, K. & Beznosova, O. (2007). On the Imbalance of the Security Problem Space and its Expected Consequences. *Information Management & Computer Security*, 15(5), 420-431.

Carlin, A., Manson, D. P., & Zhu, J. (2010). Developing the Cyber Defenders of Tomorrow with Regional Collegiate Cyber Defense Competitions (CCDC). *Information Systems Education Journal*, 8(14), 1-10.

Cetron, M. J., Davies, O., Steele, S. F., & Ayers, C. E. (2009). World War 3.0: Ten Critical Trends for Cybersecurity. *The Futurist*, 43(5), 40-49.I

Cernak, E. (2016). Top Cyber Threats can Shift by Industry, but Risk is Universal. *Property & Casualty*, 360.

Cha, Victor. (2016). Cyber Attacks on Commercial Banks Likely Linked to North Korea. *Center for Strategic and International Studies*. Retrieved on May 31, 2016, from https://www.csis.org/analysis/cyber-attacks-commercial-banks-possibly-linked-north-korea.

Colesniuc, D. (2013). Cyberspace and Critical Information Infrastructures. *Informatica Economica Journal*, 17(4), 123.

CISSP. (2015). CISSP Domains. (ISC)2. https://www.isc2.org/cissp-domains/default.aspx.

Crook, J. R. (2011). White House and Department of Defense Announce Strategies to Promote Cybersecurity, Including Strengthening Norms Affecting Internet Security. *The American Journal of International Law*, 105(4), 794-797.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research*, 20(1), 79-98, 155, & 157.

Edwards, D. (2010). Robust ICSs Critical for Guarding Against Cyber Threats. *American Water Works Association Journal*, 102(11), 30-33.

Elkind, P. (2015). Inside the Hack of the Century: Part 1. *Forbes.com*. Retrieved July 1, 2015, http://fortune.com/sony-hack-part-1/.

Fulton, E., Lawrence, C., & Clouse, S. (2013). White Hats Chasing Black Hats: Careers in IT and the Skills Required to get There. *Journal of Information Systems Education*, 24(1), 75-80.

Gabberty, J. W. (2013). Educating the Next Generation of Computer Security Professionals: The Rise and Relevancy of Professional Certifications. *The Review of Business Information Systems (Online)*, 17(3), 85-98.

Ghiglieri, M. & Stopczynski, M. (2016). SecLab: An Innovative Approach to Learn and Understand Current Security and Privacy Issues. In *Proceedings of the 17th Annual Conference on Information Technology Education* (SIGITE '16). ACM, New York, NY, 67-72.

Hannabuss, S. (2000). Being Negligent and Liable: A Challenge for Information Professionals. *Library Management*, 21(6), 316-329.

Harris, A. L., Lang, M., Yates, D., & Kruck, S.E. (2011). Incorporating Ethics and Social Responsibility in IS Education. *Journal of Information Systems Education*, 22(3), 183-189.

Healey, J. (2011). The Spectrum of National Responsibility for Cyberattacks. *The Brown Journal of World Affairs*, 18(1), 57-70.

Hill, M. (2003). Surfing, Scrolling Help get the "Battle" Rolling; Cyber Defense Exercise: The Drill Includes Computer Specialists from Military Academies, along with other Institutions. *Telegraph - Herald*, April 27, 2003, D11.

Kelly, B. B. (2012). Investing in a Centralized Cybersecurity Infrastructure: Why "Hacktivism" can and should Influence Cybersecurity Reform. *Boston University Law Review*, 92(5), 1663-1711.

Kim, S. & Choi, M. (2002). Educational Requirement Analysis for Information Security Professionals in Korea. *Journal of Information Systems Education*, 13(3), 237-248

Kington, T. (2008). A Dangerous Web Defending Against Cyber Attacks is a Growing Concern. *C4ISR*, 23.

Lewis, J. A. (2016). Russia and the DNC Hacks. *Center for Strategic and International Studies*. August 15, 2016, https://www.csis.org/analysis/russia-and-dnc-hacks.

Macaskill, E. & Dance, G. (2013). NSA Files: Decoded. *The Guardian*. November 1, 2013, http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1.

Manson, D. & Carlin, A. (2011). A League of our Own: The Future of Cyber Defense Competitions. *Communications of the IIMA*, 11(2), 1-11.

Morgan, S. (2016). One Million Cybersecurity Job Openings in 2016. *Forbes.com*. January 2, 2016, http://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/#13591eda7d27.

Morgan, S. (2015). Cybersecurity Job Market to Suffer Severe Workforce Shortage. *CSO*. July 28, 2015, http://www.csoonline.com/article/2953258/it-careers/cybersecurity-job-market-figures-2015-to-2019-indicate-severe-workforce-shortage.html.

Mulligan, D. K. & Schneider, F. B. (2011). Doctrine for Cybersecurity. *Daedalus*, 140(4), 70-92.

National Research Council (U.S.). (2009). Committee on Science, Security, and Prosperity. Beyond "Fortress America": National Security Controls on Science and Technology in a Globalized World. *Committee on Science, Security, and Prosperity [and] Committee on Scientific Communication and National Security, Development, Security, and Cooperation, Policy and Global Affairs, National Research Council of the National Academies*.

NYU Polytechnic School of Engineering. (2014). World's Biggest Student Cyber Security Competition Comes to Brooklyn. *PR Newswire*. http://www.prnewswire.com/news-releases/worlds-biggest-student-cyber-security-competition-comes-to-brooklyn-282258351.html.

Paglieri, J. (2015). Ex-NSA Director: China has Hacked 'Every Major Corporation' in U.S. *CNN Money (online)*. March 16, 2015, http://money.cnn.com/2015/03/13/technology/security/chinese-hack-us/.

PR Newswire (2016). University of Central Florida Becomes Winningest National Collegiate Cyber Defense champion. April 24, 2016, http://www.prnewswire.com/news-releases/university-of-central-florida-becomes-winningest-national-collegiate-cyber-defense-champion-300256502.html.

Rursch, J. A., Luse, A., & Jacobson, D. (2010). 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), 71-79.

Serapiglia, A. (2016). The Case for Inclusion of Competitive Teams in Security Education. *Information Systems Education Journal*, 14(5), 25-33.

Slusky, L. & Partow-Navid, P. (2012). Teaching Information Assurance Online. *The Review of Business Information Systems (Online)*, 16(2), 53-66.

Thales. (2010). Protecting National Security from Increasingly Complex Security Challenges and Threats. *Thales Group*. https://www.thalesgroup.com/en/content/protecting-national-security-increasingly-complex-security-challenges-and-threats.

Thales. (2013). Good Cyber is Good Business: The Competitive Advantage of Cyber Security. *Thales Group*. https://www.thalesgroup.com/sites/default/files/asset/document/cyber-security-audit-test-and-compliance.pdf .

U.S. Army. (2011). U.S. Army Cadets Win Retooled Cyber Competition. *C4ISR*, 10.

U.S. News & World Report. (2016). Information Security Analyst. *U.S. News & World Report: Careers*. http://money.usnews.com/careers/best-jobs/information-security-analyst.

White, G. B. & Dodge, R. C. (2006). The National Collegiate Cyber Defense Competition. *Proceedings of the 10th Colloquium for Information Security Education*. 68-74, 2006, Adelphi, MD.

AUTHOR BIOGRAPHIES

Amy B. Woszczynski is Professor of Information Systems at Kennesaw State University. She earned a Bachelor's in Industrial Engineering from Georgia Tech, an M.B.A. from Kennesaw State University, and a Ph.D. from Clemson University. She publishes on topics related to information systems education, culture, and gender, in journals such as *Journal of Information Systems Education*, *Journal of Global Information Technology Management*, *Journal of Computer Information Systems*, *International Journal of Information Management*, *Industrial Management & Data Systems*, and *Computers in Human Behavior*.

Andrew Green is Lecturer of Information Security and Assurance at Kennesaw State University. He earned a B.S. and M.S. in Information Systems from Kennesaw State University and is currently completing a Ph.D. in Information Systems, with a concentration in Information Security, at Nova Southeastern University. He publishes on topics related to information security education and has co-authored widely used textbooks in the information security space.

APPENDIX

Cyber Defense Competition Learning Outcomes and Benefits

Students participating in the Cyber Defense competition go through preparation with mentors and are then judged based on their performance in a simulated event. We are investigating the student learning outcomes associated with the preparation for the competition and the competition itself.

The results will remain anonymous and confidential except as required by law. We will not release the results in any individually identifiable manner. You may stop the survey or withdraw from the study at any time. There are no known dangers from taking the survey. By learning more about cyber defense competitions, we will be able to make recommendations to improve education over time, which will benefit students, employers, and society. The survey will take about 15 minutes to complete.

I certify that I am at least 18 years of age, and I agree to take this survey.

Are you: Judge Mentor Other _____

Part 1: Please rate how prepared you believe students are for each of the following.

Topic	Not at all Prepared	Somewhat Prepared	Moderately Prepared	Very Prepared
Access control				
Attacks on critical infrastructure				
Business continuity and disaster recovery planning				
Computer forensics				
Cryptography				
Current information security topics				
Cyberterrorism				
Economics of security				
Ethics				
Global information security				
Hacktivists				
Incident response				
Information assurance				
Information security governance				
Information security policies				
Information technology security				
Intrusion detection				
Investigation and compliance				
Legal regulations				
Linux fundamentals				
Malware				
Operations security				
Organized crime and information security				
Penetration testing				
Phishing				
Physical (environmental) security				
Physical access controls				
Politics and security				
Privacy				
Professional conduct				
Professional negligence and liability				
Providing network availability (i.e., email, file transfer, chat, phone, etc.) during a simulated attack				
Risk management				
Securing IT intellectual property rights				
Securing the interconnected organization				
Security architecture and design				
Security education, awareness, and training programs				

Security usability				
Shoulder surfing				
Social engineering				
Software development security				
Telecommunications and network security				
Windows fundamentals				
Other (please describe)				

Part 2: Please rate how important it is for students to understand each topic if they plan to pursue university/technical school education.

Part 3: Please rate how important it is for students to understand each topic if they plan to seek employment related to information security.

Part 4: Please rate how important it is for students to understand each topic if they plan to join the military.

Topic	**Not at all Important**	**Somewhat Important**	**Moderately Important**	**Very Important**
Access control				
Attacks on critical infrastructure				
Business continuity and disaster recovery planning				
Computer forensics				
Cryptography				
Current information security topics				
Cyberterrorism				
Economics of security				
Ethics				
Global information security				
Hacktivists				
Incident response				
Information assurance				
Information security governance				
Information security policies				
Information technology security				
Intrusion detection				
Investigation and compliance				
Legal regulations				
Linux fundamentals				
Malware				
Operations security				
Organized crime and information security				
Penetration testing				
Phishing				
Physical (environmental) security				
Physical access controls				
Politics and security				
Privacy				
Professional conduct				
Professional negligence and liability				
Providing network availability (i.e., email, file transfer, chat, phone, etc.) during a simulated attack				
Risk management				
Securing IT intellectual property rights				
Securing the interconnected organization				
Security architecture and design				
Security education, awareness, and training programs				
Security usability				
Shoulder surfing				
Social engineering				

Topic	Not at all Important	Somewhat Important	Moderately Important	Very Important
Software development security				
Telecommunications and network security				
Windows fundamentals				
Other (please describe)				

Considering the preparation for and completion of this cyber defense competition, how well prepared do you believe students are for each of the following:

Future plans	Not at all prepared	Somewhat Prepared	Moderately Prepared	Very Prepared
College/university				
Technical school				
Military service				
Employment				

How could the cyber competition be improved?

How could student preparation be improved?

How could the simulated environment be made more realistic?

Do you have other comments?

We'd like to gather a few demographic details now.
Are you:
Male Female

How old are you: _____ Years Old

What is your race (please check all that apply):
American Indian or Alaskan Native
Asian or Pacific Islander
Black
White

What is your ethnicity:
Hispanic origin Not of Hispanic origin

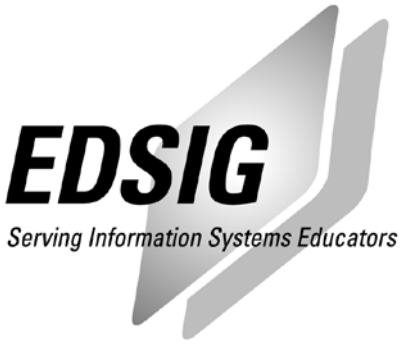
What is your job title (if retired, please list): _____

Do you currently work in:
K-12 Education Post-secondary Education (Technical school, university, etc.) Military Other ___

How many years of experience do you have in information security and related fields? _____

Would you like a copy of the results? If so, please provide your email address. Thank you for your time.

Information Systems & Computing
Academic Professionals



STATEMENT OF PEER REVIEW INTEGRITY

All papers published in the Journal of Information Systems Education have undergone rigorous peer review. This includes an initial editor screening and double-blind refereeing by three or more expert referees.

ISSN 2574-3872