Social Representations of Cybersecurity by University Students and Implications for Instructional Design

Suzanne D. Pawlowski
Information Systems & Decision Sciences Department
Louisiana State University
Baton Rouge, LA 70803, USA
spawlowski@lsu.edu

Yoonhyuk Jung
Management Track
Ulsan National Institute of Science and Technology (UNIST)
Ulsan, South Korea
yjung@unist.ac.kr

ABSTRACT

Cybersecurity has become an essential topic in introductory information systems (IS) core courses. As an aid to course design, the exploratory research in this paper uses a social representations lens to elucidate the perceptions of cybersecurity and cybersecurity threats held by students. Analysis of qualitative survey data from 152 students at a university in the Western U.S. identified 23 concepts forming the students' collective understanding of cybersecurity. Presented in the form of a social representations map, the findings reveal student perspectives that can be used to motivate and enhance learning about cybersecurity threats and mitigation strategies. Interpretation of the map indicates that students' sensemaking about cybersecurity places the strongest emphasis on technological concepts and socio-political concerns. In contrast, potential cybersecurity threats to national critical infrastructure are only minimally represented. The survey also examined students': a) level of concern about different cybersecurity threats, b) perceived likelihood they will experience given computer security incidents, and c) incidents they have already experienced. Instructors of introductory IS courses can utilize the study findings to motivate student interest by building upon topics currently evident in the representation/frame of reference and increase student awareness and attention to cybersecurity threats that are missing. Suggested instructional design approaches, tailored to the level of awareness/prior knowledge and concern indicated include: 1) a problem-centered approach for topics related to personal cybersecurity, 2) demonstrating relevance and utilizing case studies for topics on organizational cybersecurity, and 3) collaborative, guided discovery to raise awareness about national security/critical infrastructure cybersecurity threats and protections.

Keywords: Cybersecurity, Student perceptions, Social representation, Instructional pedagogy

1. INTRODUCTION

Cybersecurity has become one of the most challenging issues of the digital age. Data breaches at major retailers such as Target and Neiman-Marcus (Ramji, 2014), serious exposures in software used to secure websites and technology products such as the OpenSSL Heartbleed Bug (Hackett, 2015), and successful attacks to gain access to government agencies' data by hacktivist groups like Anonymous (Kerner, 2013) have become almost commonplace events. Surveys of the current state of cybersecurity, such as Verizon's *2015 Data Breach Investigations Report* (Verizon, 2015) which found over 100,000 confirmed security incidents in the prior year reported by 70 organizations involving 700 million compromised records and an estimated financial loss of $400 million, paint a vivid picture of the vulnerabilities of cybersecurity defenses and the relentless efforts of hackers to discover and exploit these weaknesses. New challenges and threats are continually emerging. Risk predictions for 2016, for example, include the increased spread of ransomware/cyberextortion, new vulnerabilities and threats due to the growth in cloud computing, and a wider range of security threats to industrial control systems via connected devices and networked systems through the Internet of Things (Tuttle, 2016).

As information systems (IS) educators, we are responsible for preparing our students to be aware of the risks in cyberspace, to see potential threats and to make good

decisions in their professional and personal lives. While a decade ago many colleges and universities did not include the topic of IS security in the core body of knowledge offered to their students (Rotvoid and Landry, 2007; Whitman and Mattord, 2006), today security education and training is considered essential in order to prepare students for future roles as employees, managers, business owners, and members of the boardroom. The importance given to instruction in computer/information security can be seen in calls for its inclusion as a core component of the curriculum for all IS and business students (Piazza, 2006; White, Hewitt, and Kruck, 2013) and recommendations for cybersecurity-related learning objectives/topics for the IS core course in the *IS 2010 Model Curriculum* (Topi et al., 2010) (see Table 1). To respond to this mandate, IS educators are challenged with determining how best to incorporate computer/information security content into IS core courses, updating security-related content for other classes such as systems analysis and design (Salisbury, Ferratt, and Wynn, 2015), and launching new programs to meet urgent needs for a cybersecurity professional workforce (Burley, Eisenberg, and Goodman, 2014; Foltz and Renwick, 2011; Locasto et al., 2011).

Learning Objectives	• Understand how to secure information systems resources, focusing on both human and technological safeguards • Evaluate the ethical concerns that information systems raise in society and the impact of information systems on crime, terrorism, and war

Topics	• Security of information systems
	  o Threats to information systems
	  o Technology-based safeguards
	  o Human-based safeguards
	  o Information systems security planning and management
	• Information systems ethics and crime
	  o Information privacy, accuracy, property, and accessibility
	  o Computer crime
	  o Cyberwar/cyberterrorism

Table 1. Security-related learning objectives and topics in the IS 2010 Model Curriculum – Foundations of Information Systems core course (Topi et al., 2010)

The research in this paper focuses on cybersecurity education in the IS core course, defined as "The ability to protect or defend the use of cyberspace from cyber attacks" (NIST, 2013, p. 58). Several factors make this instruction especially challenging. One issue is the rapidly changing knowledge base related to cybersecurity as technology evolves, new vulnerabilities are identified/exploited by hackers, and new mitigation strategies are developed. Perhaps an even more challenging issue is the severe constraint on lecture-time and assignments that can be devoted to security topics due to the other material that must be covered. Instructors need strategies to leverage this limited time effectively. The purpose of the research study presented in this paper is to aid IS educators in that task.

Instructional design for cybersecurity topics in the IS core course begins with establishing learning objectives and identifying the high priority topics to be covered. Going beyond this, we posit that the design of an effective learning environment for this subject matter also depends upon understanding *the perceptions of cybersecurity risks that students bring to the classroom.* Unlike some other topics in the IS core course where prior exposure has been minimal, students are not 'blank slates' when it comes to cybersecurity. Rather, they bring initial understandings that have been shaped through social interaction (media coverage, discourse, etc.) and, in some cases, personal experiences (Billig, 1996). Reports of successful hacker attacks, opinion pieces by industry pundits predicting escalating threat levels from cybersecurity breaches, and reports of diplomatic negotiations to establish cybersecurity norms have become commonplace in the media. Movies such as *Sneakers, Live Free or Die Hard,* and *Blackhat* have brought cybersecurity themes into pop culture. As students have been exposed to this discourse and engaged in dialogue with friends and family, they have formed initial understandings of cybersecurity threats that they bring to IS core courses.

Our aim in this paper is to identify the basic elements of students' sensemaking about cybersecurity risks so that IS educators can leverage this knowledge in their instructional design. By examining students' sensemaking about cybersecurity, instructors can gain a better understanding of: 1) the type of risks that are central to students' perceptions of cybersecurity and their understanding of terms related to those risks, and 2) the type of risks that are peripheral or missing from those understandings. Coverage of the types of threats where awareness is high, for example, will require less time devoted to introductory material and explanation of basic concepts. Students may also be highly motivated to deepen their understanding and to learn about the protections that can be employed to mitigate these risks. In contrast, where awareness of threats is less evident, instructors may need to adopt a different instructional approach to fill in these blind spots, cover basic concepts, and provide more examples to engage student interest and motivate learning.

For the research, we conducted an online survey of 152 students at a U.S. university to understand student sensemaking about cybersecurity risks. We used an inductive, mixed qualitative/quantitative approach utilizing social representations (Moscovici, 1981, 1984) as the theoretical foundation and analysis of similarity (Flament, 1986) as the empirical method. Social representations theory explores sensemaking processes through which social actors co-construct and share representations of social and cultural phenomena, in this case "cybersecurity." Analysis of similarity is used to identify the concepts in the representation and create a conceptual network of the organization of central and peripheral elements in those understandings. A second part of the survey explored the level of concern students had about the different types of cybersecurity threats and perceived likelihood that they would experience computer security incidents in the coming year. The framework of cybersecurity threats by Cavelty (2013) was used to formulate survey items for this part of the investigation and to aid in interpretation of the results.

The paper proceeds as follows: Social representations theory and Cavelty's (2013) framework are described in the

following section; analysis of similarity is detailed in the Method and Findings section. After presenting the results of the study, we discuss implications of the findings for the coverage of cybersecurity topics in introductory IS courses and offer preliminary suggestions for course design.

2. THEORETICAL FOUNDATION

2.1 Theory of Social Representations

A social representation is defined as "a set of concepts, statements and explanations originating in daily life in the course of inter-individual communications" (Moscovici, 1981, p. 181). Formed through social discourse (messages transmitted through tradition, education, communication media, communication with others, etc.) and experiences, they are the stock of commonsense knowledge (as opposed to scientific or expert knowledge) shared by the members of a social collective (Calafat, 1998). A social representation provides a cognitive framework to organize our thinking and action (Laroche, 1995). Social representations theory posits that the concepts forming the representation are organized into a double system: 1) a central system, or *core concepts*, that are the stable part of the representation, and 2) *peripheral concepts* that change more rapidly, adapting to specific circumstances (Abric, 1994).

Social representations theory has been used to study a wide variety of topics, including IT-related concepts such as the digital economy (Alexandra, 2001), the electronic purse (Penz, Meier-Pesti, and Kirchler, 2004), IS security in a hospital (Vaast, 2007), and electronic health records (Jung, Pawlowski, and Wiley-Patton, 2009). Social representations theory and methods are well-suited to the current inquiry, enabling elicitation and analysis of the commonsense, collective understandings of cybersecurity of university students in the U.S. The inductive approach used in the study ensured that the meanings arose from the data and not from the researchers' preconceptions of cybersecurity.

2.2 Cybersecurity Threat Representations Framework

The framework developed by Cavelty (2013) identifies three categories of cybersecurity threat representations present in discursive practices at the macro-level in the U.S. – technological, socio-political, and human-machine – and the specific threats associated with each of these clusters. Different communities of actors (e.g., hacking subculture, anti-virus industry, law enforcement, intelligence community, Homeland Security, military) are actively engaged in shaping these alternative representations which influence everyday practices of cybersecurity. As shown in Table 2, distinct sets of terms, metaphors, and other linguistic devices are associated with each of these representations. In the technological framing, for example, malware is portrayed using biological terms (virus/worms); the socio-political framing focuses on hackers of all forms; and the human-machine framing stresses the "complex interrelationships between critical infrastructures and the cyber-substructure, and a subsequent emphasis on vulnerability" (Cavelty, 2013, p. 106). While the framework is high-level, its comprehensive coverage of cybersecurity threats enabled us to see which elements of the broader discourse have been incorporated into students' sensemaking about cybersecurity.

	Technological Cluster	***Socio-Political Cluster***	***Human-Machine Cluster***
Threat	Malware • Network disruptions • Advanced persistent threats (malware)	Hackers (all kinds) • Cyber-criminals (nonstate) • Cyber-spies (state) • Cyber-terrorists (nonstate) • Cyber-commands (state)	Complexity • Disruptions in critical infrastructure • Cascading effects • (Catastro-phic) attacks on critical infrastructure
Represen-tations	Virus • Intruders • Weapons	Lawlessness • Anonymity	Vulnerability • Unknowability • Inevitability

Table 2. Cybersecurity threats/threat representations (Cavelty, 2013)

3. METHOD & FINDINGS

3.1 Data Collection and Respondent Demographics

Data for the study was collected through an online survey of students at a university in the Western region of the United States. An invitation to participate in the study was extended via e-mail to 945 students, including all Honors College students and students in 12 classes in various departments (e.g., Electrical Engineering, Psychology, Information Systems, Environmental Horticultural Science). Participation was voluntary and no incentives were provided. 152 students (16% response rate) completed the "cybersecurity" word association question; 139 of those students also completed demographic questions and questions on their level of concern about different types of cyber-threats, perceived likelihood they would experience computer security incidents in the coming year, and personal experience with computer security incidents.

As shown in Table 3, the survey respondents included undergraduate students at all levels of study as well as graduate students (Master's programs). They were overwhelmingly U.S. students; only two were international students. Business had the highest representation of the university's colleges (56%), followed by Liberal Arts (11%), Engineering (10%), Science & Mathematics (6%), Agriculture, Food & Environmental Sciences (5%), and Architecture & Environmental Design (4%) (8% did not respond to this question). When asked how often they used a computer/mobile device, all except for one participant responded Every Day.

3.2 Social Representation of "Cybersecurity"

A three-part methodology was used to create a map of the social representation of "cybersecurity" held by the students. The first step was to *elicit* the semantic universe of the social

representation using the free word association technique (Doise, Clemence, and Lorenzi-Cioldi, 1993). Free word association is used to shed light on the representation by surfacing those concepts that are most readily accessible in memory when the person thinks about the given object

College Level		
	Number	**Percentage**
Freshman	20	13.2%
Sophomore	13	8.6%
Junior	52	34.2%
Senior	40	26.3%
Graduate Student	14	9.2%
No Response	13	8.6%
Total	152	100%
Age		
	Number	**Percentage**
18 - 20	39	25.7%
21 – 22	64	42.1%
23 – 24	26	17.1%
25 – 30	8	5.2%
Over 30	1	.7%
No Response	14	9.2%
Total	152	100%

Table 3. Respondent demographics

(Abric, 1994). The second step was to *content analyze and code* the responses to determine the set of concepts in the semantic space of the representation. Finally, the results of the coding were analyzed to *identify the structure* of the representation, including the central core/periphery elements and meaningful associative chains (Abric, 2001). The analytic techniques used in this part of the analysis were Flament's (1986) *analysis of similarity* and Borgatti and Everett's (2000) *core/periphery model* to clarify the core and periphery structure.

3.2.1 Elicitation of the semantic content of the representation: The first survey question asked subjects to write down the first three words/terms or images that immediately come to mind when they see the term "cybersecurity." There were 448 responses to this question.

3.2.2 Content analysis/coding: The responses were content analyzed using an inductive process involving detailed coding and determination of thematic categories (i.e., concepts in the representation). One of the researchers first coded the data using an open coding procedure in which codes were not predetermined but emerged from the data. This yielded 92 detail codes representing the first level of abstraction of concepts present in the data. Code labels closely followed the wording used in the responses (e.g., C39 Credit Cards, C46 Affects Everyone, C80 National Defense). In cases where the response contained two subjects, multiple codes were assigned. For example, "password-protected" was assigned codes C09 Password and C47 Safety/Protection. Next, related codes were grouped into thematic categories, or topics, as shown in Table 4. Topic 7 Crime (Financial), for example, combined nine detailed codes (C64 Criminals/fraud/theft, C29 Banking, C39 Credit cards, C87 Money, and so on). (All but 40 single-instance miscellaneous responses (e.g., "hyped up," "porn") are reflected in the set of topics). A 10% sub-sample of the responses was independently re-coded by another faculty member using the set of 23 topics. The two raters were in agreement on 36 of the 46 codes in the sub-sample (consistency rate = .783; Cohen's Kappa = .762), indicating a substantial level of inter-rater reliability (Fleiss, 1981).

Topic 1	Hacker/Hacking
Topic 2	Internet
Topic 3	Safe/Secure
Topic 4	Virus/Antivirus
Topic 5	Password
Topic 6	Privacy/Surveillance
Topic 7	Crime (Financial)
Topic 8	Computer/Network
Topic 9	Firewall
Topic 10	Unsafe/Threat
Topic 11	Malware
Topic 12	IT/Technology
Topic 13	Government/Military
Topic 14	Data
Topic 15	Encryption
Topic 16	Breach
Topic 17	Security Technique (Other)
Topic 18	Unreliable
Topic 19	Tech Company
Topic 20	Cyber-terrorism
Topic 21	Cyberbullying
Topic 22	China
Topic 23	Wireless/Mobile

Table 4. Topics – Concepts in the social representation

3.2.3 Analysis of the structure of the representation: The next step in the analysis was to determine the core/periphery structure and associations among the 23 concepts (topics) in the students' semantic space for cybersecurity (Abric, 2001).

Core concepts are the quintessential components that, in combination, distinguish the social representation from similar or related representations (Tsoukalas, 2006). Abric (2001) identified three criteria for inclusion in the central core: expressive value, associative value, and symbolic value. The methodology used in this study enabled the assessment of two of these criteria – expressive and associative values - as described below. The third criterion, symbolic value, is based on the concept that central elements cannot be questioned without affecting the meaning of the entire representation. The assessment of symbolic value would require much more extensive, in-depth methods such as longitudinal studies and is beyond the scope of the present study. The representation yielded by the current analysis, therefore, should be considered a preliminary structure.

Expressive value is based on the assumption that central elements will be more frequently present in the discourse concerning the object than peripheral elements. It was assessed by the parameter *salience*, which was measured by computing the frequencies of appearance of elements (topics) in the responses (Abric, 2001; Nicolini, 1999).

Topic #	Topic	Sum of Similarity	Salience	Coreness	Membership
1	**Hacker/Hacking**	**0.785**	**73**	**0.688**	**CORE**
2	**Internet**	**0.629**	**40**	**0.384**	
4	**Virus/Antivirus**	**0.586**	**35**	**0.285**	
5	**Password**	**0.558**	**32**	**0.262**	
3	**Safe/Secure**	**0.605**	**38**	**0.245**	
6	Privacy/Surveillance	0.522	26	0.185	**PERIPHERY**
7	Crime (Financial)	0.457	25	0.178	
8	Computer/Network	0.472	22	0.174	
9	Firewall	0.336	18	0.133	
12	IT/Technology	0.252	11	0.093	
11	Malware	0.308	11	0.089	
15	Encryption	0.214	9	0.085	
10	Unsafe/Threat	0.261	15	0.082	
16	Breach	0.252	9	0.080	
13	Government/Military	0.297	9	0.072	
14	Data	0.315	9	0.065	
17	Security Technique (Other)	0.162	7	0.053	
19	Tech Company	0.250	5	0.043	
20	Cyber-terrorism	0.153	5	0.036	
22	China	0.148	4	0.035	
18	Unreliable	0.168	6	0.032	
21	Cyberbullying	0.186	5	0.031	
23	Wireless/Mobile	0.268	4	0.019	

Table 5: Core and periphery membership – Cybersecurity representation elements

Associative value assumes that central elements are associated with a larger number of elements than periphery elements. Two indexes were used to assess associative value: *sum of similarity* and *coreness*. The *sum of similarity* measure was calculated using the *analysis of similarity* method introduced by Flament (1986). An inter-attribute similarity (IAS) matrix is the fundamental component of the analysis. Each cell in the IAS matrix contains a Jaccard similarity coefficient indicating the degree of co-occurrence (proximity) for a given pair of attributes (Hammond, 1993). (The IAS matrix for this study is shown in the Appendix). Sum of similarity is calculated as the sum of the similarity coefficients of each element (topic) to all others in the IAS matrix. The higher the sum of similarity value, the closer the association of that element with the other elements.

The final parameter, *coreness*, is based on the core/periphery model by Borgatti and Everett (2000) developed to detect a core and periphery structure in network data consisting of values representing strengths of relationships among items. Coreness is considered a function of the closeness (either correlation or Euclidean distance) of an element to the center where the strength of the relationship between any two elements depends completely on the extent to which each is associated with the center (Borgatti and Everett, 2000). We used the statistical software UCINET 6.0 developed by Borgatti and colleagues to generate coreness and membership of elements in the core or periphery. The similarity index (IAS) matrix was used as the data matrix for this part of the analysis.

Salience, sum of similarity, and coreness of each topic are shown in Table 5. On the basis of the coreness measure, 5 topics were classified into the core of the social representation and the remaining 18 into the periphery. Sum of similarity and salience measures also provide support for this preliminary core/periphery structure.

3.2.4 Social representations map: In order to better understand the relationships among topics and aid in interpretation, the results were represented visually in a social representations map. The map is the 'maximum tree' of the system based on the pair-wise similarity indexes from the IAS matrix as defined by Flament (1986). Flament's (1986) notion of the 'maximum tree' is equivalent to the minimum spanning tree concept from graph theory (Doise, Clemence, and Lorenzi-Cioldi, 1993). Minimum spanning trees search for the shortest path (edge lengths) to connect all nodes in a way that there is only one link between any two nodes. Flament's 'maximum tree,' then, seeks to identify the relationships among all concepts within the network of concepts in a way that maximizes the overall similarity within the map representation. The procedure to construct the maximum tree used the nearest neighbor algorithm and three parameters drawn from the IAS matrix: (1) the pair-wise topic similarity (e.g., .110 for T1/T2); (2) the topic's salience (e.g., 73 for T1); and (3) sum of similarity of a concept to other concepts (the higher the sum of similarity the greater likelihood that the concept occupies a more central position in the map). The process was started with all 23 topics (initial X):

1. From the set of X topics, the one with the highest salience was included in the map.
2. From the set of (X-1) topics, the one with the highest similarity (highest Jaccard coefficient from the IAS

matrix) to the topic already in the map was added to the map. (If there were multiple topics with the same similarity, the one with the highest salience was picked (Kruskal, 1956). If the salience was also the same for the topics, their sum of similarity was calculated and used to break the tie.)
3. From the set of (X-2) topics, the one with the highest similarity to any of the topics already in the map was added to the map. Ties were broken as described in Step 2.
4. This iterative method was continued until all concepts were included in the map.

The map of the students' social representation of cybersecurity is shown in Figure 1.

3.2.5 Interpretation of the social representation map: Five concepts form the central core of the students' understanding of cybersecurity. (T1) *Hacker/Hacking* is the dominant concept, most frequently mentioned in responses and directly associated with three of the other four core concepts. The overwhelming majority of the student responses for this concept simply contained the terms "hacker" or "hacking," however a few responses differentiated between White Hat and Black Hat hackers. (T2) *Internet*, as the environment for hacking activities, is most closely associated with T1. Also directly associated with T1 are the core concepts (T4) *Virus/Antivirus,* representing malicious programs and the defenses against them, and (T5) *Password*. The overall objective of cybersecurity, (T3) *Safe/Secure*, is related to the other core concepts through T4.

Next highest frequency peripheral concepts most closely linked to the core are the concepts (T6) *Privacy/Surveillance* and (T7) *Crime (Financial)*. Each of these cybersecurity threats has other peripheral concepts associated with them in the representation. The largest grouping, originating from T6, reflects a variety of privacy/surveillance concerns, from T6 to (T13) *Government/Military*, to (T21) *Cyberbullying*, the networking system (T23) *Wireless/Mobile* and data protection method (T15) *Encryption*. (T22) *China* is also directly related to the privacy/surveillance concept T6. Only one peripheral concept, (T19) *Tech Company* (e.g., Google, Microsoft) is directly associated with T7. Another peripheral concept cluster is composed of negative aspects related to cybersecurity, including (T10) *Unsafe/Threat*, (T20) *Cyber-*

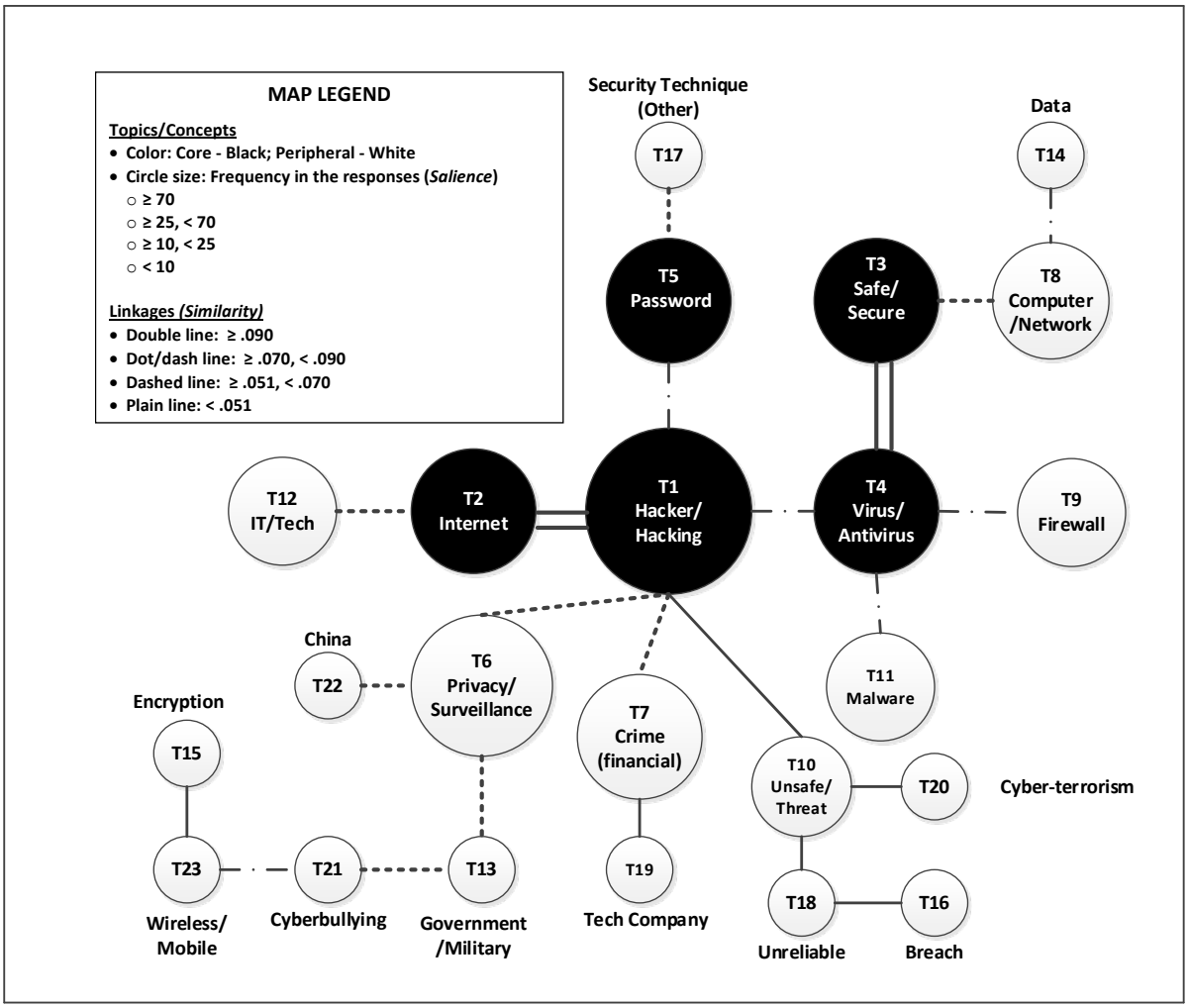

Figure 1: Students' Social Representation Map of Cybersecurity

How worried are you about the threat of cyber-attacks targeting:	Not Worried (1)	Slightly Worried (2)	Moderately Worried (3)	Very Worried (4)	*n*	Standard Deviation	Mean
1. American companies and financial institutions	23 (16.5%)	47 (33.8%)	51 (36.7%)	18 (12.9%)	139	.92	2.46
2. National critical infrastructure such as the electric grid, water and transportation systems	37 (26.6%)	44 (31.7%)	40 (28.8%)	18 (12.9%)	139	1.0	2.28
3. Classified/sensitive information maintained by the Federal Government such as data for military, diplomatic and intelligence operations	29 (20.9%)	36 (25.9%)	52 (37.4%)	22 (15.8%)	139	1.0	2.48
4. Your personal computing/mobile devices	18 (12.9%)	49 (35.3%)	48 (34.5%)	24 (17.3%)	139	.93	2.56

Table 6: Level of concern about cyber-attacks

How likely do you think it is that you will experience a computer security incident in the next year that results in the following?:	Very Unlikely (1)	Unlikely (2)	Un-decided (3)	Likely (4)	Very Likely (5)	*n*	Standard Deviation	Mean
1. Financial loss	27 (19.4%)	66 (47.5%)	30 (21.6%)	9 (6.5%)	7 (5.0%)	139	1.02	2.30
2. Exposure of personal information	12 (8.6%)	40 (28.8%)	30 (21.6%)	37 (26.6%)	20 (14.4%)	139	1.22	3.09
3. Increased level of inconvenience in your use of computers/mobile devices	14 (10.1%)	37 (26.6%)	30 (21.6%)	43 (30.9%)	15 (10.8%)	139	1.19	3.06
4. Loss of reputation	35 (25.2%)	66 (47.5%)	24 (17.3%)	10 (7.2%)	4 (2.9%)	139	.98	2.15
5. Loss of data	14 (10.1%)	46 (33.1%)	38 (27.3%)	29 (20.9%)	12 (8.6%)	139	1.13	2.85
6. Damage to personal computing/mobile devices	17 (12.2%)	50 (36.0%)	33 (23.7%)	30 (21.6%)	9 (6.5%)	139	1.13	2.74

Table 7: Likelihood of a computer incident experience in the next year

terrorism, (T18) *Unreliable,* and (T17) *Breach*. The threat (T11) *Malware* and barrier (T9) *Firewall* are associated directly with T4. A small cluster of linked general concepts, (T8) *Computer/network* and (T14) *Data*, follow from T3. Finally, (T17) *Security techniques (Other)* is directly related to T5, and (T12) *IT/Technology* is directly associated to T2. While a few of the associations are difficult to interpret, there is an apparent rationale for most of the relationships in the map.

3.3 Perceptions of Cybersecurity Threats

The survey also included questions about the student's level of concern about threats in different domains and the perceived likelihood that they would experience certain types of computer incidents in the coming year. The first question asked: *How worried are you about the threat of cyber-attacks targeting: 1) American companies and financial institutions, 2) National critical infrastructure such as the electric grid, water and transportation systems, 3)*

Classified/sensitive information maintained by the Federal Government such as data for military, diplomatic, and intelligence operations, 4) Your personal computing/mobile devices. The response scale was Not Worried (1); Slightly Worried (2); Moderately Worried (3); and Very Worried (4). The second question posed was: *How likely do you think it is that you will experience a computer security incident in the next year that results in the following?: 1) Financial loss, 2) Exposure of personal information, 3) Increased level of inconvenience in your use of computers/mobile devices, 4) Loss of reputation, 5) Loss of data, 6) Damage to personal computing/mobile devices.* A Likert-type scale for responses ranged from Very Unlikely (1) to Very Likely (5). Descriptive statistics of the responses to these two questions are shown in Tables 6 and 7.

In response to the first question (positive directionality of response categories), the students expressed a relatively modest level of concern about each of the four types of cyber-attacks, with the lowest level of concern (mean = 2.28) related to national infrastructure attacks and the highest level of concern about attacks targeting their personal computing/mobile devices (mean = 2.56). Perhaps not surprisingly, the potential threats that are more personal and visible to students generated slightly greater concern in comparison to more remote threats related to business and national security.

Replies to the second question (positive directionality of response categories) indicated low expectations by students that they would experience any of the computer security incident outcomes described in this survey question. Highest perceived likelihoods were Exposure of personal information (mean = 3.09) and Increased level of inconvenience in their use of computers/mobile devices (mean = 3.06). Perceived likelihoods of Loss of data and Damage to personal computing/mobile devices were less with means of 2.85 and 2.74, respectively. Outcomes with the lowest perceived likelihood were Financial loss (mean = 2.30) and Loss of reputation (mean = 2.15). If the range of 2.5 to 3.5 for mean outcomes is viewed as neutrality, only Financial Loss and Loss of Reputation were non-neutral and both were in the "unlikely" direction.

Finally, students were asked whether they had experienced a computer security incident within the last 12 months. Students answering Yes (23 students (17%)) were asked to briefly describe the incident(s). Students had been impacted by cybersecurity incidents that had affected a large segment of the public (e.g., Target and eBay data breaches, Heartbleed vulnerability). Credit card, PayPal, personal e-mail, and social media accounts had been hacked. Student computers were also infected by a variety of viruses and other malware.

4. DISCUSSION

By providing an initial view into student sensemaking about cybersecurity, the findings of the study suggest preliminary implications for the design of this segment of introductory IS core courses. The primary contribution of the study is that it sheds light on the view of cybersecurity and cybersecurity threats that students may bring to these classes. Faculty can use knowledge of students' frames of reference to engage them and motivate learning; to include topics that may need to be emphasized to increase student awareness; and to stimulate discussion by exploring topics where the students' points of view may differ from the perspectives of experts in the area of cybersecurity. In this section, we describe some implications for instruction based on interpretations of specific parts of the social representation and related student responses. In the following section we suggest an overall structure of coverage of cybersecurity topics, organized into three modules, each based on a different instructional approach.

To identify possible implications for the presentation of cybersecurity topics, we return to Cavelty's (2013) framework of cybersecurity threats to identify the extent to which each of the three key threat representations is evident in the students' understanding. Examination of the concepts in the social representation and detailed responses shows evidence of elements of threats/threat representations in both the "technological cluster" and the "socio-political cluster."

Once the exclusive domain of the computer security cognoscenti, technical terms such as *Malware*, *Virus/antivirus*, *Firewall,* and *Encryption* have made their way into the lexicon of the general student population. Other examples of the specialized terms present in the student responses include public keys, RSA, captcha images, WPA2, server vault, and two-factor authentication. While not all students are likely to be conversant with this vocabulary, it appears that some segment of students will have familiarity.

Cavelty's (2013) "socio-political" threat cluster focuses on hackers, and this was the central concept in the representation and most frequent response. Differentiation of types of hackers (e.g., hacker criminals, hacker spies, terrorist hackers, members of cyber-commands) can be seen in the association of the hacker concept to other elements of the representation (e.g., *Crime (Financial)*, *Cyber-terrorism*, and *Privacy/surveillance*). A few students differentiated between White Hat and Black Hat hackers and two student responses referred to the hacktivist group Anonymous. This may be one topic warranting elaboration in a course so that students understand the varied motivations, objectives, and strategies of different types of hackers. The element *China* signifies the political dimension of cybersecurity in the representation and the effect of the media in shaping perceptions. This reflects U.S. media reports that the Obama administration has strongly challenged China to curb what it contends are Chinese cyber-attacks on Americans and American companies doing business in China, and denials by senior Chinese leaders of state involvement in these activities (Barboza, 2014).

The last cluster in the framework, the "human-machine" group concerning cyber-attacks on critical infrastructure, was not evident in the students' representation of cybersecurity. It was also ranked lowest in level of concern as a target of cyber-attacks. This topic in the macro-discourse on cybersecurity spotlights threats due to system vulnerabilities in critical infrastructure and the inability to cope with adverse effects (Cavelty, 2013). Although discussions about the likelihood of cyberwar and warnings about the potential for cyber-attacks on water, power plants, and other critical systems have been frequent topics in the mainstream U.S. media over the past year and some 245 attacks on U.S. critical infrastructure were reported to the Department of

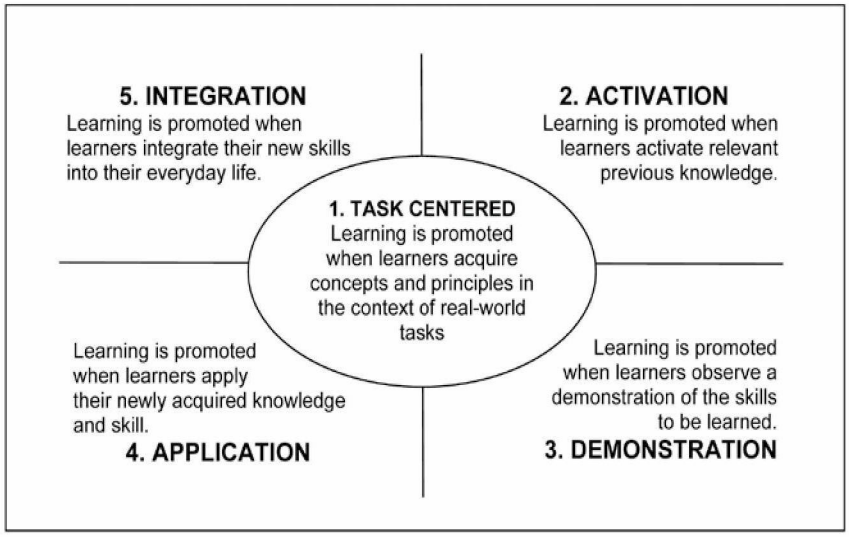

Figure 1: First principles of instruction.

Figure 2: First Principles of Instruction from Merrill (2007)

Homeland Security in 2014 (Vicinanzo, 2015), there is little evidence of student attention to these issues in the study findings. The single exception is the concept *Cyber-terrorism*. Some IS instructors may consider these topics outside of the scope of their courses, however, we believe that awareness of cybersecurity concerns from a political perspective, including calls for clearer legal and regulatory frameworks, constitutes an important dimension of digital citizenship and should be included if possible. This subject is also recommended in the IS 2010 Model Curriculum (Topi et al., 2010). As noted, these topics are not without controversy and can, therefore, provide opportunities for students to utilize and strengthen their critical thinking skills as they consider the rationales offered by different business and political actors to support various positions on these issues.

Two other observations about the content of the representation are worth noting. First is the strong presence of both optimistic (*Safe/secure*) and pessimistic (*Unsafe/threat*, *Unreliable*) views of cybersecurity. It is unclear whether this indicates that students on the whole are conflicted in this regard or is the result of individual optimistic/pessimistic biases. As this orientation has implications on cybersecurity practices, it is an intriguing question that warrants further examination. The second observation is the concern expressed about *Privacy/surveillance*. Not surprisingly, individual student responses included specific references to Edward Snowden and NSA/Prism as well as Big Brother. Clearly, this is an issue that students have attended to and warrants class discussion. Concerns about privacy and surveillance can stimulate the desire of students to deepen their understanding of the technical as well as societal aspects of cybersecurity.

5. IMPLICATIONS FOR CYBERSECURITY INSTRUCTION

In this section we build upon the findings of the study to suggest a structure and instructional approaches for the presentation of cybersecurity topics in IS core courses. The beginning point for these recommendations is the observation that student awareness, concern, and prior knowledge were significantly higher for cybersecurity threats that directly affect individuals (e.g., credit card data breaches) than for seemingly more distant concerns such as threats to organizations and national infrastructure/security. Because of these differences, we propose that different instructional approaches can provide a better fit for each type of threat domain. As detailed below, cybersecurity topics in IS core courses can be organized into three mini-modules, with each module based on a different instructional design method: 1) Personal cybersecurity risks/protections – a problem-centered instructional approach, 2) Organizational cybersecurity risks/strategies – a focus on demonstrating relevance and use of case studies, and 3) National security/critical infrastructure cybersecurity threats – collaborative guided discovery.

5.1 Personal Cybersecurity Risks/Protections: A Problem-Centered Instructional Approach (Module 1)

For cybersecurity threats that students already see as relevant to their personal lives and where they have gained some related knowledge of those risks and types of protection, the task-centered instructional approach developed by Merrill (2002, 2007) provides a good fit. The First Principles of Instruction framework developed by Merrill is shown in Figure 2. The framework aligns well to this segment of cybersecurity curriculum because of its focus on real-world problems that students already see as directly relevant to their personal lives. In addition, it also involves activating relevant previous knowledge students have about the topic.

The approach is centered on the real-world task or problem. The principles represented in the model prescribe a cycle of instruction consisting of: a) activation of prior experience, b) demonstration of skills, c) application of skills, and d) integration of these skills in the context of real-world problems/tasks (Merrill, 2002). For example, one task-centered module could focus on the protection of consumer data. Sub-topics could include identification, authentication mechanisms, passwords, and access control structure. To activate relevant previous knowledge, the instructor could

begin by facilitating a class discussion where students talk about their personal experiences with data breaches and their perceptions of the contributing causes. Encouraging students to share personal narratives about cybersecurity incidents they or those they know have experienced can heighten learning by demonstrating relevance, creating a problem-space to simulate relevant events, motivating learning, and triggering prior knowledge as a foundation for new knowledge (Swain, 2014). This might lead, for example, into a discussion of default passwords, password strength, surveys of password practices, and password encryption. For each topic set, the instructor can identify options for demonstration and application of knowledge. For passwords, for example, the instructor might discuss/demonstrate how to form a strong password; students could then form their own passwords based on the guidelines and test them using a password strength checker such as http://blog.kaspersky.com/password-check/. The integration phase of the instructional model could be a personal password 'audit' assignment where students test the strength of the types of passwords they are currently using (not using actual passwords) and then follow the guidelines learned to increase the strength, reporting before and after strength values. A next step might be to take the business perspective and strategies that can be employed for protection of users' passwords, leading to a discussion of the importance of password encryption and demonstration of encryption algorithms and discussion/demonstration of other modes of authentication.

While IS instructors may already be using some variety of these steps in the coverage of cybersecurity topics, the task-centered instructional framework provides a reminder of the value of a problem-centered approach and associated set of instructional activities. As an additional note, some researchers have begun developing and testing novel formats for instructional materials to build security knowledge and promote protection strategies in the personal computing domain. One such example is the work by Zhang-Kennedy and colleagues (2016) who created a humorous, interactive three-part comic series to help motivate learners' interest in passwords, malware protection, and mobile online privacy. That work, titled *Secure Comics*, is fully available online (http://www.versipass.com/edusec).

5.2 Organizational Cybersecurity Risks/Strategies: Demonstrating Relevance and Use of Case Studies (Module 2)

Based on the study findings, we expect that student awareness and concern for organizational cybersecurity issues will be lower than for personal computing. For this domain, the challenge for instructors is to raise the level of awareness of organizational security breaches, impacts, and avoidance/mitigation strategies. Because students will have a stronger readiness to learn when they consider that the course material is relevant to them (Knowles, Holton, and Swanson, 2012), the first challenge for instructors is to demonstrate that organizational cybersecurity is pertinent to them now and in the future. One way to generate interest in the topic and motivate them to learn more is to introduce these issues in contexts they are familiar with, such as educational settings and the types of organizations they will join in their future careers. For example, the instructor might consider inviting a member of their university's IT security team to be a guest speaker for the class. Readings could include major cybersecurity surveys such as the *Data Breach Investigations Report* published annually by Verizon, which not only identifies incident patterns and trends but also categorizes incidents by victim industry and organization size. This type of information can demonstrate to students that cybersecurity is a serious concern for their future employers. Case studies based on real-world incidents can also be a valuable teaching device to highlight the threats, vulnerabilities, and actions that lead to security incidents, as well as how they impact organizations suffering them. Cases such as the stakeholder analysis of the TJX Companies Inc. data breach by Hovav and Gray (2014), for example, can facilitate a fuller understanding of the consequences of computer security incidents. Another case appropriate for undergraduate students that uses an innovative format is the graphic novel version of *iPremier: Denial of Service Attack* by Austin and Short (2009) which raises organizational issues of risk management, crisis preparation/crisis management, and public disclosure of security risks.

5.3 National Security/Critical Infrastructure Cybersecurity Threats – Collaborative Guided Discovery (Module 3)

A third learning goal for IS core courses related to cybersecurity is to increase student understanding of the link between national security and cyberspace. Instructors face three difficult challenges related to student learning on the topic of national security/critical infrastructure cybersecurity threats. The first is low student awareness and concern about the subject, as indicated by the study findings; the second issue is the oftentimes abstruse language of discourse used to speak about these matters (e.g., cyberterrorism, cyberwar) where the precise meanings can be hard to fathom (Cavelty, 2013); the third is the complexity of the topic, which includes political and national security dimensions as well as the technical aspects related to different types of threats. Given this particular set of challenges, the instructional approach we suggest is collaborative discovery, closely guided by the instructor (Hmelo-Silver, Duncan, and Chinn, 2007).

In the collaborative mode of discovery-based learning, students work together in information-seeking, sense-making, and knowledge-building (Paul and Reddy, 2010). Using this approach to build an initial understanding of national security/critical infrastructure cybersecurity threats, the first step could be to assign each student to search for one or more recent articles on the topic in the popular media. In this way, students will be introduced different aspects of the current discourse. This task could be framed as an assignment to prepare for class discussion or as a class activity, perhaps working in small groups. The instructor can guide the inquiry by providing students with a list of example search terms, such as 'cyberwar,' 'cyberterrorism,' 'cyber weapons,' 'cyber command,' 'critical infrastructure attack,' 'cyber espionage,' 'hacktivism,' and so on. References such as *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Singer and Friedman, 2014) and *Cyber War: The Next Threat to National Security and What to Do About It* (Clarke and Knake, 2010) can be a source of

terms as well as provide instructors with additional background and varied perspectives to bring to class discussion. First, students will be asked to share what they have learned, summarizing key points in the articles they read. The instructor can facilitate the learning process by visibly recording/categorizing information during student reporting and posing questions for elaboration and clarification. The goal of this information sharing session will be to help students begin to make sense of the discourse, e.g., to understand terminology, to become aware of cybersecurity vulnerabilities/concerns as well as potential consequences, to learn about specific incidents (e.g., Stuxnet (Chen, 2010)), and to understand various viewpoints regarding threat levels, protections, and mitigation strategies. The instructor can facilitate the discussion in ways that promote critical thinking by students, adding background where needed, clarifying technical features, and so on. Open-ended discussion questions such as "What are examples of critical infrastructure that could potentially be vulnerable to cyber-attack?", "What are governments worried about and why?", "Have there been attempted and successful cyber-infiltrations into government agencies, the military, and the email accounts of government officials and other individuals with high security clearances, in the United States as well as other nations?", "How might the Internet of Things pose additional concerns?", "What steps are governments taking (or should they be taking) to address these concerns?", "What are some of the major challenges to implementing of these protections?", and "Are there different viewpoints related to…?" There is certainly no fixed set of questions or order in which they should be asked. The goal is for students to become cognitively engaged in the sensemaking and to communicate their ideas; the instructor will play a key role in facilitating the learning process and providing content knowledge on a just-in-time basis (Reynolds, 2016).

Following the discussion outlined above, the next step could be to introduce students to the types of frameworks used to reduce cyber risks to critical infrastructure. Two examples are the Cybersecurity Capability Maturity Model (C2M2) (http://energy.gov/oe/services/cybersecurity/cybersecurity-capability-maturity-model-c2m2-program) and the Framework for Improving Critical Infrastructure Cybersecurity currently under development by NIST (http://www.nist.gov/cyberframework/index.cfm).

Finally, at the conclusion of this last module, students can be made aware of the National Cybersecurity Workforce Framework, which describes cyber roles and jobs and defines the professional requirements in cybersecurity (https://niccs.us-cert.gov/training/tc/framework). This may serve to stimulate interest in careers in the field.

6. CONCLUSION

This study has provided an initial look at student perceptions of cybersecurity and threats in cyberspace and outlined a suggested instructional design for the coverage of cybersecurity topics in introductory IS classes. As an exploratory study, however, some limitations need to be noted. The primary limitation concerns generalizability. Our study explored the viewpoints of students at a single university in the U.S. at a given time. The theoretical framework of social representations highlights the social construction of meaning and constitutive effect played by messages transmitted through the communications media, the political milieu, and national culture. Given the intensity of media reporting about cybersecurity in the mainstream media in the U.S., it would not be unexpected to find strong similarities in the representations of cybersecurity of students at other U.S. universities to the representation in this study. There are, however, likely to be significant differences in the representations of cybersecurity of students in other countries, reflecting differences in media framing, cultural influences, and political systems. A second issue is a caveat based on the dynamic nature of representations (Abric, 2001). Commonsense understandings of new concepts such as cybersecurity are emergent and will continue to be influenced by changing technological developments, attempts by different political actors to shape discourse, and major computer security incidents visible to the public. The representation of cybersecurity in this study, then, provides a snapshot view at a given point in time. Both limitations noted suggest avenues for future research, including comparison of representations in different national cultures and longitudinal studies to identify changes in understandings of cybersecurity over time.

Cybersecurity education will continue to be a vital part of the preparation of every university student. Instructors of core IS courses will need to employ creative instructional approaches at the same time that they are challenged to keep current in developments in the business and political arenas related to cybersecurity as well as technical developments in order to enable their students to make good decisions in their personal and professional use of information technology. It is our hope that this study and suggested instructional approaches will provide a measure of value towards that end.

7. REFERENCES

Abric, J.-C. (1994). M´ethodologie de Recueil des Repr´esentations Sociales. in Abric, J.-C. (ed.), *Pratiques Sociales et Representations*, 59-82. Paris: Presses Universitaires de France.

Abric, J.-C. (2001). A Structural Approach to Social Representations. in Deaux, K. & Philogene, G. (eds.), *Representations of the Social: Bridging Theoretical Traditions*, 42-47. Oxford: Blackwell Publishers.

Alexandra, S. (2001). *"More and More Plugged" Social Representations of the New Economy: An Investigation into the Common Sense of Business Professionals*. Doctoral Dissertation, London School of Economics and Political Science.

Austin, R. D. & Short, J. C. (2009). *IPremier (A): Denial of Service Attack* (Graphic novel version), Product Number 609092-PDF-ENG. Boston, MA: Harvard Business School Publishing.

Barboza, D. (2014). China's President Will Lead a New Effort on Cybersecurity. *New York Times* (February 28).

Billig, M. (1996). *Arguing and Thinking: A Rhetorical Approach to Social Psychology*. Cambridge, UK: Cambridge University Press.

Borgatti, S. P. & Everett, M. G. (2000). Models of Core/Periphery Structures. *Social Networks*, 21(4), 375-395.

Burley, D. L., Eisenberg, J., & Goodman, S. E. (2014). Would Cybersecurity Professionalization Help Address the Cybersecurity Crisis? *Communications of the ACM*, 57(2), 24-27.

Calafat, A. (Ed.) (1998). *Characteristics and Social Representation of Ecstasy in Europe*. Palma de Mallorca: IREFREA-Espana.

Cavelty, M. D. (2013). From Cyber-bombs to Political Fallout: Threat Representations with an Impact in the Cyber-security Discourse. *International Studies Review*, 15(1), 105-122.

Chen, T. (2010). Stuxnet, the Real Start of Cyber Warfare? *IEEE Network*, 24(6), 2-3.

Clarke, R. A. & Knake, R. (2010). *Cyber War: The Next Threat to National Security and What to Do About It*. New York, NY: Ecco.

Doise, W., Clemence, A., & Lorenzi-Cioldi, F. (1993). *The Quantitative Analysis of Social Representations*. New York: Harvester Wheatcheaf.

Flament, C. (1986). L'Analyse de Similitude: Une Technique Pour les Recherches Sur les Representations Sociales. in Doise, W. (ed.) *L'Etude des Representations Sociales*, 139-156. Paris: Delachaux & Niestle.

Fleiss, J. L. (1981). *Statistical Methods for Rates and Proportions* (2nd Ed.). New York: John Wiley & Sons.

Foltz, C. B. & Renwick, J. S. (2011). Information Systems Security and Computer Crime in the IS Curriculum: A Detailed Examination. *Journal of Education for Business*, 86(2), 119-125.

Hackett, R. (2015). On Heartbleed's Anniversary, 3-out-of-4 Big Companies Are Still Vulnerable. *Fortune*. Retrieved April 15, 2016, from http://fortune.com/2015/04/07/heartbleed-anniversary-vulnerable/.

Hammond, S. (1993). The Descriptive Analyses of Shared Representations. in Breakwell, G. M. & Canter, D. V. (eds.), *Empirical Approaches to Social Representations*, 205-222. Oxford: Oxford University Press.

Hmelo-Silver, C. E., Duncan, R. G., & Chinn, C. A. (2007). Scaffolding and Achievement in Problem-based and Inquiry Learning: A Response to Kirschner, Sweller, and Clark (2006). *Educational Psychologist*, 42(2), 99-107.

Hovav, A. & Gray, P. (2014). The Ripple Effect of an Information Security Breach Event: A Stakeholder Analysis. *Communications of the Association for Information Systems*, 34(Article 50), 893-912.

Jung, Y., Pawlowski, S. D., & Wiley-Patton, S. (2009). Conducting Social Cognition Research in IS: A Methodology for Eliciting and Analyzing Social Representations. *Communications of the Association for Information Systems*, 24(Article 35), 597-614.

Kerner, S. M. (2013). Adobe Breach Gives Anonymous Access to Government Sites. *eWeek*.

Knowles, M. S., Holton, E. F., III, & Swanson, R. A. (2012). *The Adult Learner: The Definitive Classic in Adult Education and Human Resource Development* (7th ed.). New York, NY: Routledge.

Kruskal, J. B. (1956). On the Shortest Spanning Subtree of a Graph and the Traveling Salesman Problem. *Proceedings of the American Mathematical Society*, 7(1), 48–50.

Laroche, H. (1995). From Decision to Action in Organization: Decision-making as a Social Representation. *Organization Science*, 6(1), 62-75.

Locasto, M. E., Ghosh, A. K., Jajodia, S., & Stavrou, A. (2011). The Ephemeral Legion: Producing an Expert Cyber-security Work Force from Thin Air. *Communications of the ACM*, 54(1), 129-131.

Merrill, M. D. (2002). First Principles of Instruction. *Educational Technology Research and Development*, 50(3), 43–59.

Merrill, M. D. (2007). A Task-centered Instructional Strategy. *Journal of Research on Technology in Education*, 40(1), 5–22.

Moscovici, S. (1981). On Social Representations. in Forgas, J. (ed.), *Social Cognition: Perspectives on Everyday Understanding*,181-209. London: Academic Press.

Moscovici, S. (1984). The Phenomenon of Social Representations. in Farr, R. M. & Moscovici, S. (eds.), *Social Representations*, 3-69. Cambridge/Paris: Cambridge University Press.

Nicolini, D. (1999). Comparing Methods for Mapping Organizational Cognition. *Organization Studies*, 20(5), 833-860.

NIST (2013). *Glossary of Key Information Security Terms*, NISTIR 7298 (Revision 2), Kissel, R. (ed.). Gaithersburg, MD: National Institute of Standards and Technology.

Paul, S. A. & Reddy, M. C. (2010). Understanding Together: Sensemaking in Collaborative Information Seeking. in *Proceedings of the 2010 ACM Conference on Computer Supported Cooperative Work*, 321-330. New York, NY: Association for Computing Machinery (ACM).

Penz, E., Meier-Pesti, K., & Kirchler, E. (2004). "It's Practical, But No More Controllable": Social Representations of the Electronic Purse in Austria. *Journal of Economic Psychology*, 25(6), 771-787.

Piazza, P. (2006). Security Goes to School. *Security Management*, 50(12), 46.

Ramji, A. (2014). Thieves in Plain Sight: No One is Immune to Data Attacks. *Financial Executive*, 30(2), 104-105.

Reynolds, R. B. (2016). Relationships Among Tasks, Collaborative Inquiry Processes, Inquiry Resolutions, and Knowledge Outcomes in Adolescents During Guided Discovery-based Game Design in School. *Journal of Information Science*, 42(1), 35-58.

Rotvoid, G. & Landry, R. (2007). *Status of Security Awareness in Business Organizations and Colleges of Business: An Analysis of Training and Education, Policies, and Social Engineering Testing*. Doctoral Dissertation, University of North Dakota.

Salisbury, W. D., Ferratt, T. W., & Wynn, Jr., D. (2015). Issues and Opinions: Assessing the Emphasis on Information Security in the Systems Analysis and Design Course. *Communications of the Association for Information Systems*, 36(Article 18), 337-356.

Singer, P. W. & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford, UK: Oxford University Press.

Swain, J. (2014). Using Stories in Instructional Design. *Training & Development*, 41(5), 10-13.

Topi, H., Valacich, J. S., Wright, R. T., Kaiser, K. M., Nunamaker, Jr., J. F., Sipior, J. C., & de Vreede, G. J. (2010). *IS 2010 Curriculum Guidelines for Undergraduate Degree Programs in Information Systems.* New York, NY: Association for Computing Machinery (ACM) and Association for Information Systems (AIS).

Tsoukalas, I. (2006). A Method for Studying Social Representations. *Quality & Quantity*, 40(6), 959-981.

Tuttle, H. (2016). 10 Cyberthreat Predictions for 2016. *Risk Management Magazine*, March 1. Retrieved April 15, 2016, from http://www.rmmagazine.com/2016/03/01/10-cyberthreat-predictions-for-2016/.

Vaast, E. (2007). Danger is in the Eye of the Beholders: Social Representations of Information Systems Security in Healthcare. *Journal of Strategic Information Systems*, 16(2), 130-152.

Verizon (2015). *2015 Data Breach Investigations Report*. Retrieved April 15, 2016, from http://www.verizonenterprise.com/DBIR/2015/.

Vicinanzo, A. (2015). Sophisticated Actors Involved in Over Half of Reported Attacks on US Critical Infrastructure. *Homeland Security Today*, March 16. Retrieved April 15, 2016, from http://www.hstoday.us/single-article/sophisticated-actors-involved-in-over-half-of-reported-attacks-on-us-critical-infrastructure/2f582fa609e518caaf0aa5a358745641.html

White, G. L., Hewitt, B., & Kruck, S. E. (2013). Incorporating Global Information Security and Assurance in I.S. Education. *Journal of Information Systems Education*, 24(1), 11-16.

Whitman, M. E. & Mattord, H. (2006). *Readings and Cases in the Management of Information Security*. Boston, MA: Thomson Course Technology.

Zhang-Kennedy, L., Chiasson, S., & Biddle, R. (2016). The Role of Instructional Design in Persuasion: A Comics Approach for Improving Cybersecurity. *International Journal of Human-Computer Interaction*, 32(3), 215-257.

AUTHOR BIOGRAPHIES

Suzanne D. Pawlowski is Faculty Emeritus, Louisiana State University. She earned her Ph.D. in CIS from Georgia State University and M.B.A. and B.A. degrees from the University of California, Berkeley. Professional experience includes 20 years as a systems developer and IT manager at Lawrence Livermore National Laboratory. Scholarly publications include papers in *MISQ*, *JAIS, Information & Management* and *Database*, among others. Her current research focuses on gerontechnology, technology directed towards the aspirations and opportunities for independent living and social participation of older persons.

Yoonhyuk Jung is an Associate Professor in the School of Business Administration at Ulsan National Institute of Science and Technology (UNIST) in South Korea. He hold a PhD in Business Administration (Information Systems & Decision Sciences) from E. J. Ourso College of Business at Louisiana State University. His main research interest is users' sensemaking and adoption of emerging information technologies, with focus on digital media, mobile technology applications, and health information systems.

APPENDIX

Inter-Attribute Similarity (IAS) Matrix
(Jaccard Similarity Coefficients)

	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10	T11	T12
T1	1.000	0.110	0.039	0.085	0.074	0.052	0.054	0.039	0.034	0.038	0.022	0.030
T2	0.110	1.000	0.047	0.024	0.052	0.048	0.051	0.039	0.021	0.038	0.023	0.062
T3	0.039	0.047	1.000	0.090	0.036	0.020	0.042	0.063	0.045	0.000	0.038	0.025
T4	0.085	0.024	0.090	1.000	0.019	0.032	0.011	0.056	0.076	0.000	0.070	0.000
T5	0.074	0.052	0.036	0.019	1.000	0.045	0.074	0.047	0.053	0.000	0.014	0.000
T6	0.052	0.048	0.020	0.032	0.045	1.000	0.027	0.040	0.000	0.038	0.000	0.036
T7	0.054	0.051	0.042	0.011	0.074	0.027	1.000	0.000	0.000	0.000	0.000	0.000
T8	0.039	0.039	0.063	0.056	0.047	0.040	0.000	1.000	0.015	0.020	0.018	0.019
T9	0.034	0.021	0.045	0.076	0.053	0.000	0.000	0.015	1.000	0.000	0.022	0.023
T10	0.038	0.038	0.000	0.000	0.000	0.038	0.000	0.020	0.000	1.000	0.000	0.000
T11	0.022	0.023	0.038	0.070	0.014	0.000	0.000	0.018	0.022	0.000	1.000	0.029
T12	0.030	0.062	0.025	0.000	0.000	0.036	0.000	0.019	0.023	0.000	0.029	1.000
T13	0.030	0.025	0.000	0.014	0.000	0.059	0.021	0.000	0.000	0.000	0.000	0.000
T14	0.007	0.012	0.038	0.014	0.029	0.036	0.019	0.077	0.022	0.032	0.000	0.029
T15	0.038	0.012	0.040	0.000	0.031	0.000	0.043	0.000	0.000	0.000	0.000	0.000
T16	0.038	0.012	0.026	0.000	0.015	0.000	0.021	0.020	0.024	0.000	0.000	0.000
T17	0.015	0.026	0.014	0.000	0.051	0.020	0.000	0.000	0.000	0.000	0.036	0.000
T18	0.008	0.013	0.014	0.032	0.000	0.000	0.000	0.000	0.000	0.050	0.000	0.000
T19	0.023	0.000	0.000	0.000	0.000	0.000	0.048	0.022	0.000	0.000	0.000	0.000
T20	0.016	0.000	0.000	0.031	0.000	0.000	0.023	0.000	0.000	0.045	0.037	0.000
T21	0.016	0.000	0.000	0.016	0.018	0.000	0.000	0.000	0.000	0.000	0.000	0.000
T22	0.016	0.000	0.014	0.000	0.000	0.068	0.000	0.000	0.000	0.000	0.000	0.000
T23	0.000	0.013	0.014	0.016	0.000	0.000	0.024	0.000	0.000	0.000	0.000	0.000

	T13	T14	T15	T16	T17	T18	T19	T20	T21	T22	T23
T1	0.030	0.007	0.038	0.038	0.015	0.008	0.023	0.016	0.016	0.016	0.000
T2	0.025	0.012	0.012	0.012	0.026	0.013	0.000	0.000	0.000	0.000	0.013
T3	0.000	0.038	0.040	0.026	0.014	0.014	0.000	0.000	0.000	0.014	0.014
T4	0.014	0.014	0.000	0.000	0.000	0.032	0.000	0.031	0.016	0.000	0.016
T5	0.000	0.029	0.031	0.015	0.051	0.000	0.000	0.000	0.018	0.000	0.000
T6	0.059	0.036	0.000	0.000	0.020	0.000	0.000	0.000	0.000	0.068	0.000
T7	0.021	0.019	0.043	0.021	0.000	0.000	0.048	0.023	0.000	0.000	0.024
T8	0.000	0.077	0.000	0.020	0.000	0.000	0.022	0.000	0.000	0.000	0.000
T9	0.000	0.022	0.000	0.024	0.000	0.000	0.000	0.000	0.000	0.000	0.000
T10	0.000	0.032	0.000	0.000	0.000	0.050	0.000	0.045	0.000	0.000	0.000
T11	0.000	0.000	0.000	0.000	0.036	0.000	0.000	0.037	0.000	0.000	0.000
T12	0.000	0.029	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
T13	1.000	0.000	0.000	0.000	0.000	0.000	0.045	0.000	0.053	0.050	0.000
T14	0.000	1.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
T15	0.000	0.000	1.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.050
T16	0.000	0.000	0.000	1.000	0.000	0.050	0.045	0.000	0.000	0.000	0.000
T17	0.000	0.000	0.000	0.000	1.000	0.000	0.000	0.000	0.000	0.000	0.000
T18	0.000	0.000	0.000	0.050	0.000	1.000	0.000	0.000	0.000	0.000	0.000
T19	0.045	0.000	0.000	0.045	0.000	0.000	1.000	0.000	0.000	0.000	0.067
T20	0.000	0.000	0.000	0.000	0.000	0.000	0.000	1.000	0.000	0.000	0.000
T21	0.053	0.000	0.000	0.000	0.000	0.000	0.000	0.000	1.000	0.000	0.083
T22	0.050	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	1.000	0.000
T23	0.000	0.000	0.050	0.000	0.000	0.000	0.067	0.000	0.083	0.000	1.000

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 1055-3096