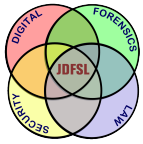

THE JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 2 | Number 1 Article 1

2007

The Common Body of Knowledge: A Framework to Promote Relevant Information Security Research

Kenneth J. Knapp
Department of Management, USAFA/DFM

F. N. Ford
Department of Management, Auburn University

Thomas E. Marshall
Department of Management, Auburn University

R. K. Rainer
Department of Management, Auburn University

Recommended Citation

Knapp, Kenneth J.; Ford, F. N.; Marshall, Thomas E.; and Rainer, R. K. (2007) "The Common Body of Knowledge: A Framework to Promote Relevant Information Security Research," *Journal of Digital Forensics, Security and Law*: Vol. 2 : No. 1 , Article 1.
DOI: https://doi.org/10.15394/jdfsl.2007.1016
Available at: https://commons.erau.edu/jdfsl/vol2/iss1/1

The Common Body of Knowledge: A Framework to Promote Relevant Information Security Research

Kenneth J. Knapp
Department of Management
USAFA/DFM
USAF Academy, Colorado USA
kenneth.knapp@usafa.af.mil

F. Nelson Ford
Department of Management
Auburn University, Alabama

Thomas E. Marshall
Department of Management
Auburn University, Alabama

R. Kelly Rainer, Jr.
Department of Management
Auburn University, Alabama

ABSTRACT

This study proposes using an established common body of knowledge (CBK) as one means of organizing information security literature. Consistent with calls for more relevant information systems (IS) research, this industry-developed framework can motivate future research towards topics that are important to the security practitioner. In this review, forty-eight articles from ten IS journals from 1995 to 2004 are selected and cross-referenced to the ten domains of the information security CBK. Further, we distinguish articles as empirical research, frameworks, or tutorials. Generally, this study identified a need for additional empirical research in every CBK domain including topics related to legal aspects of information security. Specifically, this study identified a need for additional IS security research relating to applications development, physical security, operations security, and business continuity. The CBK framework is inherently practitioner oriented and using it will promote relevancy by steering IS research towards topics important to practitioners. This is important considering the frequent calls by prominent information systems scholars for more relevant research. Few research frameworks have emerged from the literature that specifically classify the

diversity of security threats and range of problems that businesses today face. With the recent surge of interest in security, the need for a comprehensive framework that also promotes relevant research can be of great value.

Keywords: information security, common body of knowledge, research relevance, literature review

1. INTRODUCTION

Information and internet technology is automating everything from supply chains to medical records to grocery self-checkout lines. Many individuals would not know how to make their lives work nor their business profitable without information technology (Schou & Trimmer, 2004). It has reached a point where one can argue that modern economies have become fully dependent on cyber-technology for survival. Unfortunately, the increased reliance on information technology (IT) has made organizations more vulnerable to a wide variety of dangerous cyber attacks. Noticing the greater risks, many IT executives now consider computer and information security as one of their top issues. A 2003 key issues survey of members of the Society for Information Management ranked security & privacy as the third top issue (Luftman & McLean, 2004). This represents a shift compared to previous years. During the 1980s, respondents never ranked the security issue in the top ten. In 1994, the security issue dropped off the top 20 list entirely (Brancheau, Janz, & Wetherbe, 1996). Table I summarizes the key issue survey results between 1980 and 2003. A different study by the Computer Sciences Corporation concluded that, for the first time, information security topped a list of CFO concerns related to information technology (Computer Sciences Corporation, 2005). Based on these surveys, we can conclude that information security is one of the most critical information technology issues facing organizations today.

Table I. Security issue rankings published in the *MIS Quarterly*[1]

Year	Ranking
1980	#12
1986	#18
1989	#19
1994	Not ranked
2003	#3

[1] From 1980-1994, the ranked title was *security & control*. In 2003, it was *security & privacy*.

Despite the criticality of protecting organizational information, security research has not traditionally been a mainstream research topic in the information systems (IS) literature. Kotulic & Clark (2004) described IS security research as one of the more intrusive types of research and noted that empirical studies are seriously lacking. However, there is a recent surge of interest in security among IS researchers to include empirical studies. In addition to existing journals such as *Journal of Digital Forensics, Security and Law*, we are seeing new dedicated information security academic journals, special journal issues, conferences, special interests groups, curricula programs, and scholarly books (e.g. Quigley, 2004). This growth in interest has created a need for additional frameworks to help researchers classify existing literature based on the diversity of topics that exist in the security field.

Literature Search of Existing Frameworks. Considering the importance of information security today and the potential impact that relevant scholarly research can have in helping to solve critical cyber security issues, few comprehensive frameworks exist to guide researchers in selecting topics to study. Yet, there is not a lack of frameworks designed for specific purposes within the realm of information security. Existing frameworks present an architecture for network security management (Dawkins, Clark, Manes, & Papa, 2005), information security governance (Posthumus & von Solms, 2004), secure execution of software (Maña, Lopez, Ortega, Pimentel, & Troya, 2004) and offer conceptual approaches of examining information security management (Eloff & von Solms, 2000; Finne, 1998). Other frameworks in the literature present an automated structure for vulnerability notification (Al-Ayed, Furnell, Zhao, & Dowland, 2005) and use possibility theory to evaluate risk to national infrastructures (Baskerville & Portougal, 2003). Some frameworks offer a particular lens to view information security such as an ethical view (Trompeter & Eloff, 2001), an information warfare view (Cronin & Crawford, 1999; Friman, 2001; Knapp & Boulton, 2006) and a view based on analogies to biological cells (Knapp, Morris, Rainer, & Byrd, 2003). Moreover, various frameworks exist that examine different aspects of electronic commerce risk and security (Aljifri, Pons, & Collins, 2003; Kesh, Ramanujan, & Nerur, 2002; Rees, Bandyopadhyay, & Spafford, 2003). Finally, one framework examined the information security literature using a socio-philosophical approach (Dhillon & Backhouse, 2001). Overall, based on our search of information security frameworks in the scholarly literature, we did not find any comprehensive framework specifically designed to promote relevant research aimed at solving real-world information security issues.

The primary intent of this article is to demonstrate how scholars can direct research toward relevant ends by using an industry-developed framework. A secondary intent is to pinpoint topics for future IS security studies by identifying literature gaps using the CBK framework. Research frameworks

based on real-world experience can help researchers focus their studies on relevant problems. This article presents a literature review that looks back ten years to roughly the beginning of the modern Internet era. Articles on information security from ten leading IS academic journals are organized by the ten domains of the information security common body of knowledge (CBK). Referencing articles to a common body of knowledge is not new to literature reviews (Taylor & Giannantonio, 1993) and is useful in identifying specific research streams and gaps.

The subject of the relevance of academic research has received substantial discussion in a number of IS academic journals. This discussion has often come in the form of opinion pieces by some leading IS scholars. Baskerville & Myers (2004, p. 329) state that there have been, "frequent calls for IS researchers to make their research more relevant to practice (Zmud, 1998), yet it seems IS researchers continue to struggle to make excellent research practically relevant." Others have called not only for IS researchers to make their research more relevant but also to look to practitioners for the identification of topics and to look to the IS literature only after a commitment is made to a specific topic. Recommendations such as attending industry conferences, talking to practitioners, and reading practitioner journals are ways that researchers can identify relevant topics (Benbasat & Zmud, 1999). We propose that researchers interested in producing relevant research can also look to frameworks developed and maintained by practitioners as an additional way to select topics. While arguing for relevant research, we do not intend to diminish and minimize the importance of knowledge exploration in academic research where contributions tend not to be relevant to practitioners. This type of research is also needed. Yet, the need for relevant research is critical. One survey sent to 400 IS practitioners indicated that practitioners find academic research dated, difficult to read, and of little practical value (Pearson, Pearson, & Shim, 2005). To help solve this perception among practitioners, we suggest scholars make greater use of industry-developed frameworks in order to promote knowledge where research contributions address problems relevant to the practitioner community (Dennis, 2001). For this article, we demonstrate this suggestion by reviewing published information security articles from ten leading IS journals and organizing the research by the information security CBK.

The organization of the paper is now described. The next section reveals the literature review methodology used in the study. This section is followed by the results of the review. The discussion section highlights the literature gaps and research opportunities identified by using our methodology. Finally, a conclusion is provided.

2. LITERATURE REVIEW METHODOLOGY

This study analyzes information security literature from 1995 to 2004 in ten respected IS scholarly journals. Articles are organized according to an industry-developed common body of knowledge.

2.1 Ten Domains of the Common Body of Knowledge

Broadly defined, security represents the quality or state of being secure and free from dangers. To be secure is to receive protection from adversaries and other hazards (Whitman & Mattord, 2004). The importance of security often becomes critical especially in threatening and hostile environments. Information security is a more recent phenomena corresponding to the rise of computers, networks and the global Internet. Considering this growing concern, the authors searched for an industry-developed framework to organize research topics relating to the type of security threats that businesses today face. The information security common body of knowledge (CBK) served this purpose.

The International Information Systems Security Certification Consortium [(ISC)^2] is a non-profit organization that manages the CBK and the certified information system security professional (CISSP) program.[2] The CISSP is the first IT certification to be accredited under ISO/IEC 17024, a global benchmark for the certification of workers in various professions (Vijayan, 2004). This ISO certification added credibility and validity to the (ISC)^2 organization as one of the world's foremost information security certifying bodies. Among the requirements, CISSP candidates must pass a comprehensive exam to demonstrate mastery of the CBK (Hansche, Berti, & Hare, 2004). Established in 1989, the CBK has provided a shared reference for information security professionals. Described on the (ISC)^2 web site, "the (ISC)^2 CBK is a taxonomy - a collection of topics relevant to information security professionals around the world…(it) establishes a common framework of information security terms and principles which allows information security professionals worldwide to discuss, debate, and resolve matters pertaining to the profession with a common understanding." Table II lists the ten CBK domains. The Appendix B provides a short definition of each domain.

[2] *(ISC)^2, CISSP,* and the *Common Body of Knowledge (CBK)* are registered marks. See www.isc2.org. In the practitioner literature, we have seen the CBK interchangeably referred to as the CISSP CBK, the (ISC)^2 CBK, and the information security CBK.

Table II. Ten domains of the information security common body of knowledge

Information Security Management
Security Architecture & Models
Access Control Systems & Methodology
Applications & Systems Development
Operations Security
Cryptography
Physical Security
Telecommunications, Network & Internet Security
Business Continuity Planning (BCP)
Law, Investigations, & Ethics

The authors selected the CBK model over other security models (e.g. the confidentiality, integrity, and availability (CIA) triad) because of the comprehensive nature of the CBK and the expectation that specific recommendations for future research would result by using it. The CBK is inherently practitioner oriented and can guide research towards topics that are important to security practitioners. Considering the frequent calls for IS researchers to make their research more relevant as well as the recommendation of looking to practitioners to identify topics, we regard the practitioner-orientation of the framework as a strength.

2.2 Ten Years from 1995-2004

The Internet era has had a broad and profound effect on individuals, organizations, and society alike (Sampler, 2000). Expectedly, much of the information systems security research prior to the modern Internet era focused on internal security threats and ways to deter computer abuse (e.g. Straub, 1990; Straub & Goodhue, 1991; Straub & Nance, 1990). In one study, the Internet threat is briefly mentioned as a growing source for computer system abuse (Straub & Welke, 1998).

While computer security-related issues have been important to businesses since dependence on computers first started (Martin, 1973), this review limits articles to those published since the beginning of the modern Internet era.

Analyzing the size of the Internet can approximate when this era began. From January 1995 to January 1996, the number of Internet hosts grew from 5.8 to 14.4 million, a one year increase of 248% (Internet Systems Consortium, 2005). No year since 1995 has experienced this degree of growth. Considering that research published in 1995 was likely conducted prior to or during 1994, the 1995 cut-off date for this review seems appropriate to mark the beginning of the modern Internet era.

2.3 Ten Leading IS Journals.

Ten journals were selected for this review based on a ranking of top IS research publication outlets (Peffers & Ya, 2003, p72). The selected publications represent a wide range of outlets within the IS academic domain. All ten journals have been respectfully ranked in other rankings (e.g. Lowry, Romans, & Curtis, 2004, p53). Journals were limited to those classified as 'pure IS research' and thus we did not include 'allied' publications such as *Communications of the ACM, Decision Sciences,* and *Computers & Security* (Peffers & Ya, 2003) in our review. Considering our primary purpose of demonstrating how scholars can use an industry-developed framework, such as the $(ISC)^2$ CBK, to direct research toward relevant ends, focusing on ten leading IS journals provides an adequate base for our study. Later in the results section, we present a list of the journals included in this study.

2.4 Heuristics for Article Inclusion

Having decided to organize IS security articles from ten journals over a ten-year period according to the CBK model, a search for candidate articles began. An extensive key word search of common IS security terms was conducted that included using key words from each of the ten domains in the CBK (e.g. encryption, business continuity). Academic search engines were used (e.g. EBSCO) and each journal's table of contents was scanned to find articles not caught by the database searches (Webster & Watson, 2002). In doing so, the first author scanned 2,848 article citations from the ten selected journals. Using both database searches and scans of tables of contents, 93 candidate articles were collected for consideration.[3]

Once the candidate articles were identified, two heuristics were developed to select the articles in this study. The first heuristic called for inclusion if the term *security* or substitute terms such as *information assurance* appeared in the article title, abstract, or key words. This heuristic alone, however, did not produce a sufficient number of articles for the review. To expand the list, a second heuristic was developed for articles that did not meet the first heuristic yet contained one of the ten CBK domain topics in the title, keywords, or abstract. For example, we identified articles that addressed CBK domain

[3] The list of the 93 initial articles is available from the first author.

topics such as law, ethics, access control and applications development. Then, if the article addressed the CBK domain topic *primarily* from an information security perspective, the article was included. This decision involved a qualitative judgment based on a reading of the article and a frequency analysis of the term 'security' and related terminology in the text and reference titles. Generally, the more frequent these terms appeared, the more likely the article was included. Using this approach, the first two authors independently judged which articles to include in this study and agreed on the classification of 86 of the 93 initial articles. The differences in opinion were resolved through a discussion to arrive at an agreed decision.

The method used for article selection excluded some related works to our phenomena of interest. For example, *An Empirical Examination of the Concern for Information Privacy Instrument* (Stewart & Segars, 2002) investigated the subject of information privacy. This article could potentially fit into the CBK domain of *law, investigations, and ethics*. However, an evaluation of the article revealed that it did not address the privacy topic from primarily a security perspective; the term 'security' did not appear once in the article text or references. Based on this evaluation, we agreed not to include the article in this review. In contrast, the article *Internet Privacy – At Home and At Work* (Boncella, 2001) was included in the review. While this article did not meet the conditions of the first heuristic, the term 'security' appeared seven times including in the article's introduction. Based on this and a reading of the article, we agreed that the article addressed the privacy topic from a security perspective and thus included it in the review.

2.5 Classification Criteria

Once included, each article was classified in two ways. First, each was cross-referenced to one or two of the ten domains of the CBK. This classification was based on the topics addressed in the title, keywords, and abstract as well as the body of the article. Second, each article was identified as tutorial/conceptual (T), methodology/framework (M), or empirical research (E). Publications that we reviewed that were not empirical research but provided a tutorial or focused on a single concept or topic we classified as tutorial/conceptual pieces (T). This classification is appropriate for our study considering the large number of tutorial articles identified in the literature. Publications that were not empirical research but proposed a security methodology, model or framework we classified as methodology/framework (M). Finally, publications providing the results of empirical research we appropriately classified as empirical (E). Identical to the selection process, the first two authors independently classified each article. In instances when opinions differed, a discussion determined the optimum classification.

The following section presents the results of applying the research methodology described in this section. A discussion of the results will follow.

3. RESULTS

This literature study identifies IS security articles between 1995 and 2004 in ten leading IS journals. We initially selected 93 candidate IS security articles, representing 3% of the total articles in the ten journals. Of the 93 articles, 48 met the condition of the first or second heuristic described in the previous section. Table III provides a tally by journal of both the candidate and the included articles for this study. Table IV breaks down the 48 selected articles by year published. Appendix A provides the complete list of the 48 selected articles classified by article type and cross-referenced to the CBK.

Table III. IS Security Articles per Journal (1995-2004)

Journal by rank order (Peffers & Ya, 2003)	Candidate	Included
MIS Quarterly	5	2
Information Systems Research	7	3
Journal of MIS	8	3
European Journal of IS	3	1
Information and Management	19	13
Communications of the AIS	17	14
Decision Support Systems	16	9
Database	7	0
Journal of the AIS	5	1
Information Systems Journal	6	2
Total	93	48

Table IV. Articles by Year

Year	Number of Articles
1995	1
1996	2
1997	2
1998	4
1999	2
2000	7
2001	7
2002	6
2003	5
2004	12
Total	48

4. DISCUSSION

An advantage of using the industry-developed CBK to classify information security literature is that it requires us to organize literature using a framework designed primarily for practitioners. This approach helps the researcher to align academic literature with a practitioner framework that can result in identifying gaps and streams in the literature. Researchers can then consider embarking on studies that investigate these areas since they are important to practitioners. In the case of the $(ISC)^2$ CBK, we assume that all ten domains are valuable and critical information security areas that contain rich topics for the IS researcher to consider. While some of the CBK domains may at first glance seem more appropriate for other, non-IS disciplines (e.g. cryptography for the computer science discipline; law and investigations for the legal discipline), we believe all ten domains have considerable research potential for the IS researcher. For example, the public key infrastructure topic is best classified under the CBK domain of 'cryptography' (see International Information Systems Security Certification Consortium, 2002), yet this topic has and should continue to present viable research opportunities for IS researchers. Thus, we recommend researchers take an inclusive approach to all of the domains of the CBK framework by not excluding any as being outside the bounds of potential IS research.

The 48 articles selected for this review represent the most security-focused articles in ten leading IS journals. Upon examining Appendix A, a number of research streams and gaps are apparent. Clearly, the *security architecture and models* and the *telecommunication, network, and internet security* are the two dominant domains with nearly 80% of the 48 articles categorized into one or both of these domains. Thus, while not diminishing the importance of additional research in these two domains, a finding of this study is that there is a general need for additional research in the other eight domains of the CBK.

Within and across individual domains, a few streams can be identified. First, we identified eight articles covering the topic of information privacy & trust, representing the largest stream within the confines of our study (Boncella, 2001; Fernandes, 2001; Henderson & Snyder, 1999; Klang, 2001; Koufaris & Hampton-Sosa, 2004; Liu, Marchewka, Lu, & Yu, 2004; Srivastava & Mock, 2000; Stafford & Urbaczewski, 2004). Second, we identified six articles about the burgeoning topic of e-commerce security (Boncella, 2000; Cheng, 2000; Farhoomand & McCauley, 2001; Gupta, Stahl, & Whinston, 1998; Khazanchi & Sutton, 2001; Rohm & Pernul, 2000). Finally, we identified four research studies that used deterrence theory in a significant part of the article (Gopal & Sanders, 1997; Harrington, 1996; S. M. Lee, Lee, & Yoo, 2004; Straub & Welke, 1998). It is noteworthy that the use of deterrence theory in IS security research is a stream that began well before the contemporary Internet age. For example, earlier IS literature covering security management focused on

countermeasures, deterrence, and abuse prevention (Hoffer & Straub, 1989; Parker, 1981; Straub & Nance, 1990).

Much of the empirical work on IS security predates the onset of the Internet era with security research still in the early states of development (see Bento & Bento, 2004). As noted earlier, some have described empirical information security research as seriously lacking partly because of the intrusive nature of this type of research as well as the general mistrust that exists when an outsider attempts to research the activities of security practitioners (Kotulic & Clark, 2004). The results of this study support the impression that empirical research in information security is generally lacking in the IS literature in at least the ten IS journals included in this review. Fifty-eight percent of the articles in this review were identified as non-empirical, consisting mostly of tutorials, methodologies and frameworks. Some of the empirical studies used secondary data (Bagchi & Udo, 2003; Bento & Bento, 2004) while others that attempted primary data collection suffered from low sample sizes (e.g., Kotulic & Clark, 2004). Nevertheless, this study identified twenty empirical articles. Although generally in short supply, these empirical articles, along with articles from other journals not included in this review, can serve as a useful foundation for future empirical research in IS security.

The CBK framework pointed to a few obvious gaps in the reviewed literature. Foremost, the study did not classify a single article from the selected journals that addressed the CBK areas of 1) *operations security*, 2) *physical security* or 3) *business continuity planning* as a main topic of the article. These domains undoubtedly have dimensions worth researching when considering relevant topics such as the ever-decreasing size of memory devices and the risks they pose (Raikow, 2004), the pervasive use of information technology in the general security field such as in airport security (Arnone, 2005), and the call for appropriate business continuity preparation in disaster planning (9/11 Commission, 2004). We believe these three CBK domains offer many opportunities for relevant IS research.

Our review categorized only three articles in the *applications and systems development* domain. It is surprising that there are not more security articles in this area considering that information systems development is considered a mainstream IS topic which has been part of traditional IS curricula for years (Gorgone et al., 2002). In addition, the fifteen articles in the *security management* domain is a relatively small number. Based on the argument that most security problems require managerial rather than technical solutions (Panko, 2004), we believe there is still a great need for IS security management studies. This finding is consistent with the Dhillon & Backhouse (2001, p.148) call for additional empirical research to "develop key principles for the prevention of negative events and therefore to help in the management of security."

Overall, in the IS journals selected for this review, there are few articles that *exclusively* research information security. However, by looking for articles that address IS security as an important component of the article, there is a larger number of articles worth considering. Although not heavily researched, IS security nevertheless has been an important topic in some of the leading IS journals. Based on our review, the two journals that published the most security articles serve very different needs of the diverse IS research community. *Communications of the AIS* published fourteen of the articles in this review with nine categorized as tutorials. In contrast, *Information & Management* published thirteen of the articles with ten categorized as empirical research.

This study has limitations. First and perhaps most important, our examination included ten journals and is not intended to be a comprehensive review of all IS security literature. Yet starting with a list of ten leading IS journals is appropriate considering that many consider the major contributions in scholarly research to be in these journals (Webster & Watson, 2002). Reviewing other outlets within and outside the IS community is necessary to appreciate the full body of security literature. Future uses of the CBK model can be applied to different sets or even individual journals. For example, a future study could apply the CBK model to all the security literature published in *Journal of Digital Forensics, Security and Law*. Second, many articles did not easily fit into the classification scheme provided by the CBK and other articles covered multiple topics and could have appropriately been categorized in more than two domains. However, selecting two CBK domains captured the primary topic for each article. Third, our second heuristic for article inclusion was based on subjective judgment. Although rigor was used to ensure a reliable and valid process, some may disagree with the decision to include or not include certain articles.

The advantages of using the information security CBK are substantial. First, the CBK framework is inherently practitioner oriented and using it can therefore promote relevancy by steering IS research towards topics important to practitioners. Second, the CBK provides a comprehensive framework that identifies a wide range of research opportunities for the IS scholar and helps us to consider topics that IS researchers may not traditionally consider (e.g. business continuity). Also, the CBK is not a static framework because the $(ISC)^2$ organization is free to modify the domains as the state and needs of the industry change. Third, the framework is extendible to evaluate security research in other journals and timeframes. Moreover, as the number of IS security articles increases, future literature reviews can focus on single or selected domains within the CBK. Finally, the $(ISC)^2$ CBK is only one practitioner oriented framework that can be used to organize scholarly literature. Instead of the CBK, researchers could use other frameworks such as the ISO 17799 in a way similar to how we used the CBK in this literature review (see ISO/IEC, 2005).

5. CONCLUSION

This article uses the information security common body of knowledge as a framework to organize published IS research. Developed and maintained by practitioners, the CBK framework can be used by IS researchers to guide future studies towards topics that are relevant to the information security industry. By applying this framework to 48 articles from 1995 to 2004 in ten leading IS journals, this study identified a general need for additional empirical research in every CBK domain and particularly in the domain of IS security management. Additionally, this study identified a large need for additional security research relating to IS applications development, physical security, operations security, and business continuity. This article demonstrates how scholars can use an industry-developed framework to organized literature that can result in directing research toward relevant ends.

6. REFERENCES

9/11 Commission. (2004). The 9/11 commission report - final report of the national commission on terrorist attacks upon the united states (Authorized, First ed.). New York: W. W. Norton & Company.

Al-Ayed, A., Furnell, S. M., Zhao, D., & Dowland, P. S. (2005). An automated framework for managing security vulnerabilities. Information Management & Computer Security, 13(2/3), 156-166.

Aljifri, H. A., Pons, A., & Collins, D. (2003). Global e-commerce: A framework for understanding and overcoming the trust barrier. Information Management & Computer Security, 11(2/3), 130-138.

Arnone, M. (2005, May 16). Airport security enters a new phase. Federal Computer Week. Retrieved May 19, 2005, from www.fcw.com/article88687-04-25-05-web

Backhouse, J., & Dhillon, G. (1996). Structures of responsibility and security of information systems. European Journal of Information Systems, 5(1), 2-9.

Bagchi, K., & Udo, G. (2003). An analysis of the growth of computer and internet security breaches. Communications of the AIS, 12(46), 684-700.

Baskerville, R. L., & Myers, M. D. (2004). Special issue on action research in information systems: Making IS research relevant to practice. Forward. MIS Quarterly, 28(3), 329-335.

Baskerville, R. L., & Portougal, V. (2003). A possibility theory framework for security evaluation in national infrastructure protection. Journal of Database Management, 14(2), 1-13.

Benbasat, I., & Zmud, R. W. (1999). Empirical research in information systems: The practice of relevance. MIS Quarterly, 23(1), 3-16.

Bento, A., & Bento, R. (2004). Empirical test of a hacking model: An exploratory study. Communications of the AIS, 14(32), 678-690.

Boncella, R. J. (2000). Web security for e-commerce. Communications of the AIS, 4(11), 1-42.

Boncella, R. J. (2001). Internet privacy - at home and at work. Communications of the AIS, 7(14), 269-282.

Boncella, R. J. (2002). Wireless security: An overview. Communications of the AIS, 9(15), 269-282.

Boncella, R. J. (2004). Web services and web services security. Communications of the AIS, 14(18), 344-363.

Brancheau, J. C., Janz, B. D., & Wetherbe, J. C. (1996). Key issues in information systems management: 1994-95 SIM results. MIS Quarterly, 20(2), 225-242.

Cavusoglu, H., Cavusoglu, H., & Raghunathan, S. (2004). Economics of IT security management: Four improvements to current security practices. Communications of the AIS, 14(3), 65-75.

Cheng, E. C. (2000). An object-oriented organizational model to support dynamic role-based access control in electronic commerce. Decision Support Systems, 29(4), 357-369.

Computer Sciences Corporation. (2005). Information security tops list of CFO concerns. Retrieved June 9, 2005, from http://www.csc.com/newsandevents/news/4042.shtml

Cronin, B., & Crawford, H. (1999). Information warfare: Its applications in military and civilian contexts. Information Society, 15(4), 257-264.

Dawkins, J., Clark, K., Manes, G., & Papa, M. (2005). A framework for unified network security management: Identifying and tracking security threats on converged networks. Journal of Network & Systems Management, 13(3), 253-267.

Dennis, A. R. (2001). Relevance in information systems research. Communications of the AIS, 6(10), 1-6.

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: Towards socio-organizational perspectives. Information Systems Journal, 11(2), 127-153.

Eloff, M. N., & von Solms, S. H. (2000). Information security management: A hierarchical framework for various approaches. Computers & Security, 19(3), 243-256.

Farhoomand, A., & McCauley, M. (2001). Tradecard: Building a global trading electronic payment system. Communications of the AIS, 7(18), 1-37.

Fernandes, A. D. (2001). Risking "trust" in a public key infrastructure: Old techniques of managing risk applied to new technology. Decision Support Systems, 31(3), 303-322.

Finne, T. (1998). A conceptual framework for information security management. Computers & Security, 17(4), 303-307.

Friman, H. (2001). A systems view of information warfare. Journal of Information Warfare, 1(1), 25-32.

Gavish, B., & Gerdes, J. H., Jr. (1998). Anonymous mechanisms in group decision support systems communication. Decision Support Systems, 23(4), 297-328.

Gopal, R. D., & Sanders, G. L. (1997). Preventive and deterrent controls for software piracy. Journal of Management Information Systems, 13(4), 29-47.

Gorgone, J. T., Davis, G. B., Valacich, J. S., Topi, H., Feinstein, D. L., & Longenecker, H. E., Jr. (2002). IS 2002 model curriculum and guidelines for undergraduate degree programs in information systems. Communications of the AIS, 11(1), 1-63.

Gupta, A., Stahl, D. O., & Whinston, A., B. (1998). Managing computing resources in intranets: An electronic commerce perspective. Decision Support Systems, 24(1), 55-69.

Gupta, A., Tung, Y. A., & Marsden, J. R. (2004). Digital signature: Use and modification to achieve success in next generation e-business processes. Information & Management, 41(5), 561-575.

Hansche, S., Berti, J., & Hare, C. (2004). Official $(ISC)^2$ guide to the CISSP exam. New York: Auerbach.

Harrington, S. J. (1996). The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. MIS Quarterly, 20(3), 257-278.

Henderson, S. C., & Snyder, C. A. (1999). Personal information privacy: Implications for MIS managers. Information & Management, 36(4), 213-220.

Hoffer, J. A., & Straub, D. W. (1989). The 9 to 5 underground: Are you policing computer crimes? Sloan Management Review, 35-43.

International Information Systems Security Certification Consortium. (2002). CISSP certification common body of knowledge study guide. Framingham, MA: $(ISC)^2$.

Internet Systems Consortium. (2005). Internet domain survey. Retrieved May 1, 2005, from www.isc.org

ISO/IEC. (2005). Information technology - code of practice for information security management (No. ISO/IEC 17799:2005): The International Standards Organization/The International Electrotechnical Commission.

Jung, B., Han, I., & Lee, S. (2001). Security threats to internet: A Korean multi-industry investigation. Information & Management, 38(8), 487-498.

Kesh, S., Ramanujan, S., & Nerur, S. (2002). A framework for analyzing e-commerce security. Information Management & Computer Security, 10(4), 149-148.

Khazanchi, D., & Sutton, S. G. (2001). Assurance services for business-to-business electronic commerce: A framework and implications. Journal of the Association for Information Systems, 1(11), 1-55.

Kim, J., Lee, J., Han, K., & Lee, M. (2002). Business as buildings: Metrics for the architectural quality of internet businesses. Information Systems Research, 13(3), 239-254.

Klang, M. (2001). Who do you trust? Beyond encryption, secure e-business. Decision Support Systems, 31(3), 293-301.

Knapp, K. J., & Boulton, W. R. (2006). Cyber warfare threatens corporations: Expansion into commercial environments. Information Systems Management, 23(2), 76-87.

Knapp, K. J., Morris, R., Rainer, K. R., Jr., & Byrd, T. A. (2003). Defense mechanisms of biological cells: A framework for network security thinking. Communications of the AIS, 12(47), 701-719.

Koh, C. E., & Watson, H. J. (1998). Data management in executive information systems. Information & Management, 33(6), 301-312.

Kotulic, A. G., & Clark, J. G. (2004). Why there aren't more information security research studies. Information & Management, 41(5), 597-607.

Koufaris, M., & Hampton-Sosa, W. (2004). The development of initial trust in an online company by new customers. Information & Management, 41(3), 377-397.

Kwok, S. H., Cheung, S. C., Wong, K. C., Tsang, K. F., Lui, S. M., & Tam, K. Y. (2002). Integration of digital rights management into the internet open trading protocol. Decision Support Systems, 34(4), 413-425.

Kwok, S. H., Yang, C. C., Tam, K. Y., & Wong, J. S. W. (2004). SDMI-based rights management systems. Decision Support Systems, 38(1), 33-46.

Lee, S., & Han, I. (2000). Fuzzy cognitive map for the design of EDI controls. Information & Management, 37(1), 37-50.

Lee, S. M., Lee, S. G., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. Information & Management, 41(6), 707-718.

Liao, Z., & Cheung, M. T. (2002). Internet-based e-banking and consumer attitudes: An empirical study. Information & Management, 39(4), 283-295.

Liu, C., Marchewka, J. T., Lu, J., & Yu, C.-S. (2004). Beyond concern: A privacy-trust-behavioral intention model of electronic commerce. Information & Management, 42(1), 127-142.

Lowry, P. B., Romans, D., & Curtis, A. (2004). Global journal prestige and supporting disciplines: A scientometric study of information systems journals. Journal of the Association for Information Systems, 5(2), 29-77.

Luftman, J., & McLean, E. R. (2004). Key issues for IT executives. MIS Quarterly Executive, 3(2), 89-104.

Maña, A., Lopez, J., Ortega, J. J., Pimentel, E., & Troya, J. M. (2004). A framework for secure execution of software. International Journal of Information Security, 3(2), 99-112.

Martin, J. (1973). Security, accuracy, and privacy in computer systems. Englewood Cliffs, NJ: Prentice-Hall.

Panko, R. R. (2003). Slammer: The first blitz worm. Communications of the AIS, 11(12), 207-218.

Panko, R. R. (2004). Corporate computer and network security. New Jersey: Prentice Hall.

Parker, D. B. (1981). Computer security management. Reston, Virginia: Reston Publishing Company.

Payne, C. (2002). On the security of open source software. Information Systems Journal, 12(1), 61-78.

Pearson, M. J., Pearson, A., & Shim, J. P. (2005). The relevancy of information systems research: The practitioner's view. Information Resources Management Journal, 18(3), 50-67.

Peffers, K., & Ya, T. (2003). Identifying and evaluating the universe of outlets for information systems research: Ranking the journals. Journal of Information Technology Theory and Application, 5(1), 63-84.

Post, G., & Kagan, A. (2000). Management tradeoffs in anti-virus strategies. Information & Management, 37(1), 13-24.

Posthumus, S., & von Solms, R. (2004). A framework for the governance of information security. Computers & Security, 23(8), 638-646.

Quigley, M. (2004). Information security and ethics: Social and organization issues. Hershey, PA: IRM Press.

Raikow, D. (2004, July 9). Do small devices equal big threat? eWeek. Retrieved May 19, 2005, from www.eweek.com/article2/0,1759,1621784,00.asp

Rees, J., Bandyopadhyay, S., & Spafford, E. H. (2003). PFIRES: A policy framework for information security. Communications of the ACM, 46(7), 101-106.

Rohm, A. W., & Pernul, G. (2000). COPS: A model and infrastructure for secure and fair electronic markets. Decision Support Systems, 29(4), 343-355.

Ryan, S. D., & Bordoloi, B. (1997). Evaluating security threats in mainframe and client/server environments. Information & Management, 32(3), 137-146.

Sampler, J. L. (2000). The internet changes everything (ICE) age. In R. W. Zmud (Ed.), Framing the domains of IT management (pp. 209-220). Cincinnati, Ohio: Pinnaflex Educational Resources, Inc.

Sarathy, R., & Muralidhar, K. (2002). The security of confidential numerical data in databases. Information Systems Research, 13(4), 389-403.

Schou, C. D., & Trimmer, K. J. (2004). Information assurance and security. Journal of Organizational and End User Computing, 16(3), i-vii.

Srivastava, R. P., & Mock, T. J. (2000). Evidential reasoning for webtrust assurance services. Journal of Management Information Systems, 16(3), 11-32.

Stafford, T. F., & Urbaczewski, A. (2004). Spyware: The ghost in the machine. Communications of the AIS, 14(15), 291-306.

Stewart, K. A., & Segars, A. H. (2002). An empirical examination of the concern for information privacy instrument. Information Systems Research, 13(1), 36-49.

Straub, D. W. (1990). Effective IS security: An empirical study. Information Systems Research, 1(3), 255-276.

Straub, D. W., & Goodhue, D. L. (1991). Security concerns of system users. A study of perceptions of the adequacy of security. Information & Management, 20(1), 13-27.

Straub, D. W., & Nance, W. D. (1990). Discovering and disciplining computer abuse in organizations: A field study. MIS Quarterly, 14(1), 45-60.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. MIS Quarterly, 22(4), 441-469.

Sundararajan, A. (2004). Managing digital piracy: Pricing and protection. Information Systems Research, 15(3), 287-308.

Taylor, S. M., & Giannantonio, C. M. (1993). Forming, adapting, and terminating the employment relationship: A review of the literature from individual, organizational, & interactionist perspectives. Journal of Management, 19(2), 461-515.

Thuraisingham, B. (1995). Multilevel security for information retrieval systems. Information & Management, 28(1), 49-61.

Trompeter, C. M., & Eloff, J. H. P. (2001). A framework for the implementation of socio-ethical controls in information security. Computers & Security, 20(5), 384-392.

Varshney, U. (2003). Wireless i: Mobile and wireless information systems: Applications, networks, and research problems. Communications of the AIS, 12(11), 155-166.

Vijayan, J. (2004, June 28). ISO endorses key security certification. Computerworld, 38, 1-2.

Volonino, L., Gessner, G. H., & Kermis, G. F. (2004). Holistic compliance with sarbanes-oxley. Communications of the AIS, 14(11), 219-233.

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. MIS Quarterly, 26(2), xii-xxiii.

Whitman, M. E., & Mattord, H. J. (2004). Management of information security. Cambridge, MA: Course Technology - Thompson Learning.

Whitworth, B., & Zaic, M. (2003). The WOSP model: Balanced information system design and evaluation. Communications of the AIS, 12(17), 258-282.

Yemini, Y., Dailianas, A., Florissi, D., & Huberman, G. (2000). Marketnet: Protecting access to information systems through financial market controls. Decision Support Systems, 28(1/2), 205-216.

Zmud, R. (1998). Editor's comments. MIS Quarterly, 22(2), xxxix-xxxii.

Zviran, M., & Haga, W. J. (1999). Password security: An empirical study. Journal of Management Information Systems, 15(4), 161-185.

APPENDIX A: INFORMATION SECURITY ARTICLES ORGANIZED BY THE COMMON BODY OF KNOWLEDGE

Shortened Title (Author, Year)	Article Type[4]	Arch & Models	Telecom, Network, Internet	Info Sec Mngt	Law, Invest, Ethics	Access Control	Apps & Sys Dev	Crypto	Phys Sec	Busi Cont Plan	Ops Sec
Multilevel security (Thuraisingham, 1995)	M	X				X					
Structures of responsibility & security (Backhouse & Dhillon, 1996)	M			X							
Codes of ethics and personal denial of responsibility (Harrington, 1996)	E			X	X						
Threats Mainframe & Client/Server (Ryan & Bordoloi, 1997)	E	X		X							
Controls for software piracy (Gopal & Sanders, 1997)	E	X			X						
Data management in EIS (Koh & Watson, 1998)	E					X	X				
Security planning models (Straub & Welke, 1998)	E	X		X							
Computing resources in intranets (Gupta et al., 1998)	M	X	X								
Anonymous mechanisms (Gavish & Gerdes, 1998)	M	X						X			
Personal information privacy (Henderson & Snyder, 1999)	M			X	X						
Password security (Zviran & Haga, 1999)	E					X					
Design of EDI controls (S. Lee & Han, 2000)	E		X	X							

[4] T = Tutorial, Conceptual M = Methodology, Frameworks E = Empirical

APPENDIX A (CONTINUED): INFORMATION SECURITY ARTICLES ORGANIZED BY THE COMMON BODY OF KNOWLEDGE

Shortened Title (Author, Year)	Article Type	Arch & Models	Telecom, Network, Internet	Info Sec Mngt	Law, Invest, Ethics	Access Control	Apps & Sys Dev	Crypto	Phys Sec	Busi Cont Plan	Ops Sec
Anti-virus strategies (Post & Kagan, 2000)	E		X	X							
Web security for e-commerce (Boncella, 2000)	T	X	X								
COPS: model for secure markets (Rohm & Pernul, 2000)	M	X		X							
Access control in e-commerce (Cheng, 2000)	M		X			X					
Access through financial controls (Yemini, Dailianas, Florissi, & Huberman, 2000)	M	X				X					
WebTrust assurance services (Srivastava & Mock, 2000)	M	X	X								
Assurance services for B2B commerce (Khazanchi & Sutton, 2001)	E	X	X								
Global trading payment system (Farhoomand & McCauley, 2001)	E	X	X								
Risking "trust" in a public key infrastructure (Fernandes, 2001)	T				X			X			
Beyond encryption, secure e-business (Klang, 2001)	T			X	X						
Current directions in IS security research (Dhillon & Backhouse, 2001)	M	X		X							

APPENDIX A (CONTINUED): INFORMATION SECURITY ARTICLES ORGANIZED BY THE COMMON BODY OF KNOWLEDGE

Shortened Title (Author, Year)	Article Type	Arch & Models	Telecom, Network, Internet	Info Sec Mngt	Law, Invest, Ethics	Access Control	Apps & Sys Dev	Crypto	Phys Sec	Busi Cont Plan	Ops Sec
Internet privacy: home & work (Boncella, 2001)	T		X		X						
Security threats to internet-Korean (Jung, Han, & Lee, 2001)	E		X								
Internet-based e-banking (Liao & Cheung, 2002)	E		X								
Architectural quality of internet businesses (Kim, Lee, Han, & Lee, 2002)	E	X	X								
Wireless security (Boncella, 2002)	T		X								
Digital rights management into Open Trading Protocol (Kwok et al., 2002)	M	X	X								
Open source software (Payne, 2002)	E	X					X				
Confidential numerical data (Sarathy & Muralidhar, 2002)	M	X				X					
Defense of biological cells (Knapp et al., 2003)	M	X	X								
Analysis of security breaches (Bagchi & Udo, 2003)	E		X								
Slammer: Blitz worm (Panko, 2003)	T		X								
Mobile and wireless information systems (Varshney, 2003)	T	X	X								

APPENDIX A (CONTINUED): INFORMATION SECURITY ARTICLES ORGANIZED BY THE COMMON BODY OF KNOWLEDGE

Shortened Title (Author, Year)	Article Type	Arch & Models	Telecom, Network, Internet	Info Sec Mngt	Law, Invest, Ethics	Access Control	Apps & Sys Dev	Crypto	Phys Sec	Busi Cont Plan	Ops Sec
Balanced IS design and evaluation (Whitworth & Zaic, 2003)	M			X			X				
Web services security (Boncella, 2004)	T		X			X					
Economics of IT security mgt (Cavusoglu, Cavusoglu, & Raghunathan, 2004)	T	X		X							
Spyware: The ghost in the machine (Stafford & Urbaczewski, 2004)	T		X		X						
Why there aren't more security studies (Kotulic & Clark, 2004)	E			X							
Social control and general deterrence (S. M. Lee et al., 2004)	E	X		X							
Digital signature (Gupta, Tung, & Marsden, 2004)	M		X					X			
Privacy-trust behavioral intention (Liu et al., 2004)	E	X	X								
Hacking model (Bento & Bento, 2004)	E	X	X								
Compliance with Sarbanes-Oxley (Volonino, Gessner, & Kermis, 2004)	T			X	X						
SDMI-based rights management (Kwok, Yang, Tam, & Wong, 2004)	M				X	X					

APPENDIX A (CONTINUED): INFORMATION SECURITY ARTICLES ORGANIZED BY THE COMMON BODY OF KNOWLEDGE

Shortened Title (Author, Year)	Article Type	Arch & Models	Telecom, Network, Internet	Info Sec Mngt	Law, Invest, Ethics	Access Control	Apps & Sys Dev	Crypto	Phys Sec	Busi Cont Plan	Ops Sec
Initial trust in an online company (Koufaris & Hampton-Sosa, 2004)	E	X	X								
Managing digital piracy: pricing and protection (Sundararajan, 2004)	M	X			X						
Totals	T=11 M=17 E=20	25	24	15	10	8	3	3	0	0	0

APPENDIX B: (ISC)^2 COMMON BODY OF KNOWLEDGE (CBK®)

Abridged from Hansche, Berti, and Hare (2004)

CBK Domain	Description
Information Security Management	The identification of an organization's information assets and life cycle management of policies, standards, procedures, and guidelines. Tools such as awareness training and risk assessments are used to identify threats and implement effective security controls.
Security Architecture and Models	The concepts, principles, structures, and standards used to design, implement, monitor, and secure systems, equipment, networks, and applications. Used in controls that enforce various levels of availability, integrity, and confidentially.
Access Control Systems and Methodology	Outlines options that control access to an organization's information and data processing resources. Emphasis is on various administrative, physical, and technical/logical controls.
Applications and Systems Development	Pertains to security concepts that apply during software development, operation, and maintenance processes.
Operations Security	Identifies the operational controls over hardware, media, and the operators and administrators with access privileges to these resources. The safeguarding of assets associated with the data processing environment.
Cryptography	Addresses the principles, means, and methods of disguising information to ensure its integrity, confidentiality, and authenticity.
Physical Security	The protection of valuable information assets of the entire business enterprise facility.
Telecommunication, Network, and Internet Security	The structures, transmission methods, transport formats, and security measures used to provide protection of transmission over private and public communications networks and media.
Business Continuity Planning	The capability to process a critical business system in the event of disruption to normal business operations.
Law, Investigations, and Ethics	Computer crime laws and regulations, investigative measures and techniques, and ethical codes of conduct for the security professional.

ABOUT THE AUTHORS

Dr. Kenneth J. Knapp is an assistant professor of management at the U.S. Air Force Academy, Colorado. His publications include *Information Management & Computer Security, Communications of the Association for Information Systems, Information Systems Management, and Information Systems Security.* He has forthcoming publications in the *International Journal of Information Security & Privacy* and *Information Security Management Handbook* 2007 and 2008 editions.

Dr. F. Nelson Ford is an Associate Professor of Management Information Systems at Auburn University, Alabama. He has published in journals such as *MIS Quarterly, Journal of Management Information Systems*, and *Information & Management*. His research interests include decision support systems and the principles of scholarship.

Dr. Thomas E. Marshall is an Associate Professor of MIS, Department of Management, Auburn University, Alabama. He is a CPA and has been a consultant in the area of accounting information systems for over 20 years. His publications include *Information & Management*, *Information Systems Security, Information Management & Computer Security, Journal of Computer Information Systems*, *Journal of End User Computing*, *Information Resource Management* and *Journal of Database Management*.

Dr. R. Kelly Rainer, Jr. is George Phillips Privett Professor of MIS, Department of Management, Auburn University, Alabama. He received his Ph.D. from the University of Georgia and has published in leading academic and practitioner journals. His most recent book is Introduction to Information Systems (1e) coauthored with Efraim Turban and Richard Potter.