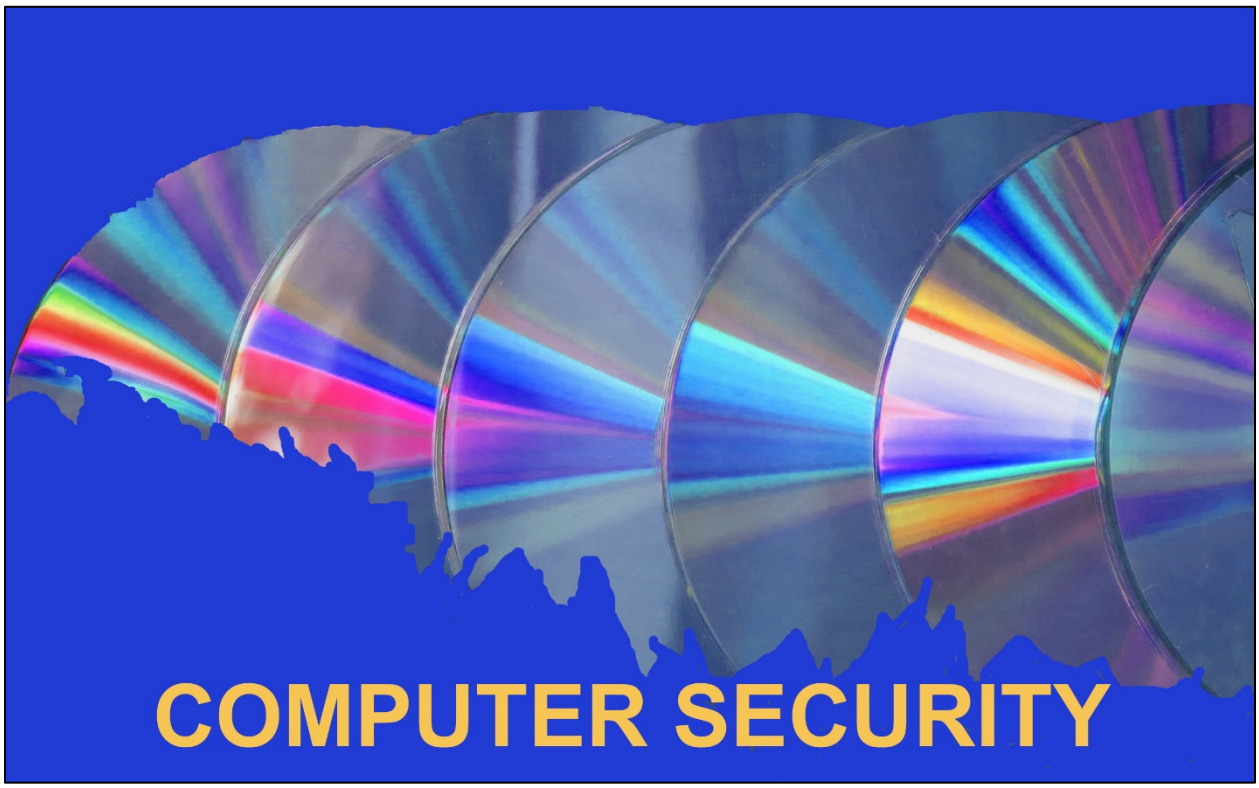
“Hackers are already at work exploiting a newly discovered flaw in Microsoft’s Internet Explorer that has left more than half of the world’s Web browsers vulnerable to attack, including those on many federal government computers.”
***The Washington Post*, April 28, 2014.**



IN THE INTRODUCTORY BUSINESS INFORMATION SYSTEMS COURSE: A FOLLOW-UP STUDY OF TEXTBOOK COVERAGE

By Kenneth J. Sousa, Laurie E. MacDonald, and Kenneth T. Fougere

Peer Reviewed

Kenneth J. Sousa ksousa@bryant.edu, Laurie E. MacDonald, and Kenneth T. Fougere are members of the faculty of the Department of Computer Information Systems at Bryant University.

ABSTRACT

The authors conducted a study of MIS textbooks as a follow-up to a study completed in 2005 and found, as in the earlier study, that computer security receives limited depth of coverage in the textbooks. Textbooks continue to publish a variety of topics and issues relating to technology security. A comparison of the results of the previous and current research studies clearly indicate there is additional coverage. This increase illustrates the importance of security topics and issues for students completing an introductory information systems course. The research they conducted also suggests that MIS faculty need to provide additional material to supplement textbook coverage in order to provide adequate coverage of this serious issue.

INTRODUCTION

The need for computer security is unquestioned in today's world where all aspects of societal activity depend on information technology. Whether it be processing business transactions, a wide variety of educational pursuits, keeping up with the latest news, leisure activities such as gaming, or simply staying in touch with family and friends, it seems that everything we do is dependent on information technology. According to the Bureau of Labor Statistics, the economy of the United States and its users rely on computer systems (Anonymous "Occupational Outlook Handbook"). Neither the government nor private sector could function today without the use of technology.

A recent study found that 56% of the respondents were confronted with a data breach in the preceding two years (Sposito). A 2013 research study commissioned by Symantec, consisting of 277 companies in nine countries, validates the increase in data breaches (Chaudhary). The number of attacks is also becoming more commonplace. A study by the Ponemon Institute reported that the surveyed organizations reported 102 successful attacks per week, with 1.8 attacks per company (Anonymous *2012 Cost of Cyber Crime Study: United States*). The most common crimes listed in the study were caused by denial of service, malicious insiders or web-based attacks.

The economic cost of cybercrimes continues to be very costly. A 2012 study completed by The Ponemon Institute found that the average annualized cost of cybercrimes is $8.9 million (Anonymous *2012 Cost of Cyber Crime Study: United States*). The study stated that the range of costs for the 56 organizations included in the study ranged from $1.4 million to $46 million in 2011. After an incident involving a credit card data breach by TJ Maxx, legislation in Massachusetts was passed which required organizations to self-report along with potential fines per incident (Bednar). Therefore,

the costs associated with cybercrimes include potential fines and liability as well as the direct cost of responding and mitigating attacks.

Computer security is a constantly evolving discipline and is now an integral part of all information system operations (Potter). Examples of the need for IT security were displayed and presented at the 2012 DEFCON Hackers conference. One security expert demonstrated that mobile devices can be readily hacked and may result in giving the attacker access to an organization's entire IT system. The security flaws in routers from the Chinese company Huawei were discussed at length along with the vulnerabilities presented by bugs in software to support virtual servers (Kirk).

The growing popularity of cloud computing as platforms, for both business and consumers, has introduced another layer of security concerns and potential attacks (Cheng). Cloud computing technology is still developing and there remains some confusion about exactly what cloud computing means and exactly what security risks are involved. It is expected that the deployment of applications to cloud computing will increase. A recent report by Gartner predicts that cloud computing will be the bulk of information technology expenditures by 2016 (Anonymous "Gartner: Cloud Will Be Bulk of It Spending by 2016").

While the benefits are believed to be high, the security risks posed may also be significant and may prevent some from entering the cloud (Anonymous "Congress Addressed on Cloud Computing Security, Opportunities and Risks"; Vaquero, Rodero-merino and Morán). The 2010 Global IT Risk Study by IBM's Institute for Business Value found that 77% of respondents felt that cloud computing increased the difficulty of privacy protection and 50% were concerned about a possible data breach. These concerns found that businesses increased their reluctance to adopt cloud services. While cloud-based services can provide increased security over their in-house systems, it is clear that businesses must carefully consider whether to store critical information such as credit card account information using this method (Greenwald). To focus on these important concerns, IBM has launched a project initiative aimed directly at improving cloud security (Anonymous "IBM Targets Cloud Computing with Security Infrastructure, Services"). The goal of the project is to provide security help to both users of cloud computing and cloud service providers.

Problem Statement

Studies have shown a dramatic increase in the number of information security breaches resulting in major financial losses and economic impact worldwide. There has been a concomitant increase in investments in information security (Chang and Wang). In addition, it has been found that both graduate and undergraduate students do not exhibit an understanding of effective information security behaviors and do not properly apply information security tools (Mensch and Wilkie; Sousa, MacDonald and Fougere).

Therefore, it is very appropriate that regardless of the career path chosen by college students, proficiency with computer applications is a fundamental requirement. Humans still remain the weakest link in computer security (Au). In today's information

security environment, they will also need a basic understanding of computer security issues and procedures.

Research Objective

Given this situation and the changing technology environment, the researchers revisited and updated the work done on a previous project (Sousa, MacDonald and Fougere). A comprehensive review of introductory management information systems (MIS) textbooks was conducted to study the level of information security coverage. The objective of this research would be to replicate the previous study and analyze the changes over the last seven years of textbooks published. This research study will compile four data points in order to assess its findings: 1) table of contents, 2) index, 3) page count and 4) depth/quality of coverage. The conclusions from this research may provide some insight into the trajectory of security coverage in academic textbooks as well as some guidance for both textbook authors and educators.

METHODOLOGY

This research study was designed to revisit the issue of the depth of coverage of information systems security topics in introductory MIS textbooks and update the results of a previous study (Sousa, MacDonald and Fougere). There is a wide range of terminology used to describe information security issues. Therefore, to structure a framework for our discussion, a set of keywords was developed to identify security issues. In order to provide continuity and enable a comparison with the earlier study, we adopted the same set of keywords used in that study. The keyword list was developed after reviewing security textbooks (Erbschloe; Volonino and Robinson; Whitman and Mattford) and web sites devoted to computer security (Anonymous "Develop a Computer Deployment Plan That Includes Security Issues"; Anonymous "Introduction to Risk Analysis"; Anonymous "ISO 177799 Directory").

Data Compilation

Four categories were defined to group the keywords in order to facilitate data analysis and regularize the data. The keyword categories are: (1) Security Threats, (2) Risk Management, (3) Security Education, and (4) Security Technology. For example, spoofing, viruses, and worms are categorized under the common rubric of security threats. The security categories are defined in Table 1 below.

TABLE 1

SECURITIES CATEGORIES

Category	Definition
Security Threats • Hackers • Denial of Service • Malicious Code	A person, group, or entity that poses an ongoing danger to one or more information assets (Holden; Whitman and Mattford).

Category	Definition
• Social Engineering • Spoofing • Trojan Horse • Viruses • Worms	
Risk Management • Continuity Planning • Disaster Recovery • Incident Response Team • Security Planning • Security Vulnerabilities • Data Integrity • Risk Assessment	Identifying security threats and acting to eliminate or at least minimize the impact on your Information assets (Anonymous "Introduction to Risk Analysis"; Anonymous "ISO 177799 Directory"; Erbschloe).
Security Education • Security Awareness • Security Procedures • Security Training • Computer Threats	Ensure that staff understand the need for security and are prepared to make security an integral part of the job (Volonino and Robinson; Whitman and Mattford).
Security Technology • Cryptography • Firewall • Network Security • Password Management • Virus Scanning	Technology designed to guard against threats to information assets (Anonymous "Develop a Computer Deployment Plan That Includes Security Issues"; Erbschloe; Holden).

Textbook Portfolio Compilation

Nine MIS instructors (four Full Professors and five Associate Professors) were asked to provide a list of the MIS textbooks they had used or reviewed recently. In addition, textbook publishers were contacted to provide additional textbooks to supplement our textbook research portfolio. Based on this list, the researchers were able to collect a representative sample of MIS textbooks. The final textbook portfolio, as shown in Appendix A, is representative of those textbooks used in an introductory MIS course.

Data Collection and Analysis

The methodology to analyze the textbook portfolio was based on the technique employed by MacDonald and Fougere and Sousa et al (Sousa, MacDonald and Fougere). The analysis team comprised three Computer Information Systems (CIS) faculty: (1) a Full Professor with 20 years industry experience and 31 years teaching CIS, (2) a Full Professor with 17 years industry experience and 32 years teaching CIS,

and (3) an Associate Professor with 15 years industry experience and 19 years teaching CIS.

Each member of the data collection team worked independently to analyze each of the textbooks. As previously defined, the security categories and associated keywords, were formatted to build a data collection form to ensure consistency during the textbook analysis. The procedure consisted of the following tasks used in the earlier study (Sousa, MacDonald and Fougere):

- Table of Contents: Identified each term that was included in the table of contents. Each keyword identified in the TOC was noted on the data collection form with a “Y” accordingly.
- Index: Identified each term that was included in the index. As each instance of the keyword was identified, the page references were logged on the data collection form in the respective column.
- Page Count: Logged the number of pages associated with the security topic.
- Quality of Coverage: Read the textbook material presented for each keyword and conducted a heuristic evaluation of the quality of the concept’s coverage. The reviewer was asked to assign an evaluation of the quality of the coverage.

When a textbook included significant coverage of any security content, that issue would appear as chapter and/or section headings in the table of contents (Bachrach); no such entry indicates minimal discussion of the issue. Consequently, a reader will be able to locate specific topics discussed in a textbook by using the textbook’s index . The researchers examined the table of contents and index for each textbook in the textbook portfolio and recorded the page numbers for each topic. The textbook material was independently read by each reviewer and an evaluation ranking was assigned using a four-point, forced Likert scale (Anonymous "Likert Scaling"). The researchers evaluated the material for the depth and quality of coverage that would provide a basic understanding of information security.

A summary of unique page references was made for each keyword to eliminate any “*double-counting*” of multiple citations within a category. The data was analyzed to determine the mean page count devoted to each keyword category, regardless of whether a category was cited in the index, and whether or not a category was cited in the table of contents. The result of this analysis provided the foundation for the research findings and conclusions.

RESULTS

UPDATED 2012 STUDY

An analysis of the table of contents for each content area was assembled to show the percent of textbooks with a respective citation. As illustrated in Figure 1, each

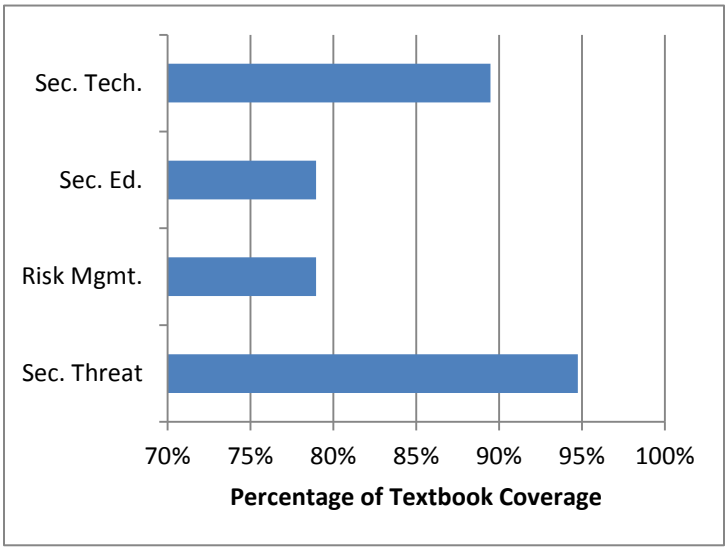


Figure 1 – Analysis of Table of Contents

of the content areas was identified in more than 75% of the sample textbooks. The security threat content area was covered in almost all of the textbooks (94%). The security technology area was highly covered in the textbooks, but at a smaller rate (89%). The remaining two coverage areas were covered less, both at (79%). However, it is clear that each of the topics were significantly depicted in the table of contents for the textbook population.

The table of contents analysis provided some insight into the coverage of topics. Its perspective provided only a limited, narrow inclusion at a high-level for a conceptual

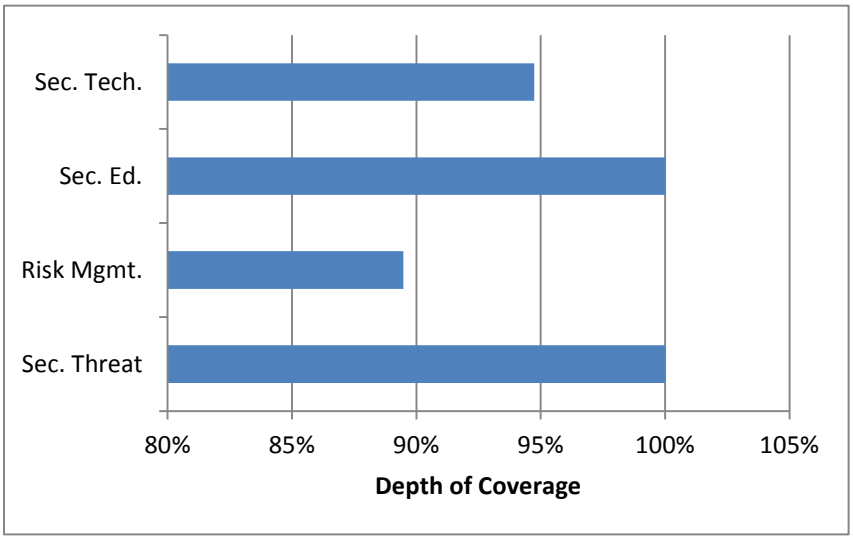


Figure 2 – Analysis of Index Citations

topic. Therefore, it was important to supplement the analysis with the depth of coverage. The research gathered additional data, as shown in Figure 2, to “drill down” with the actual coverage of subordinate, related topics. The index citations were examined in

detail. If the citation was found to relate directly to one of the four content areas, it was assigned to that content area as shown in the figure.

The table of contents and index analysis data, by itself, do not provide a complete perspective relating to the coverage of textbook content. The “depth” of the

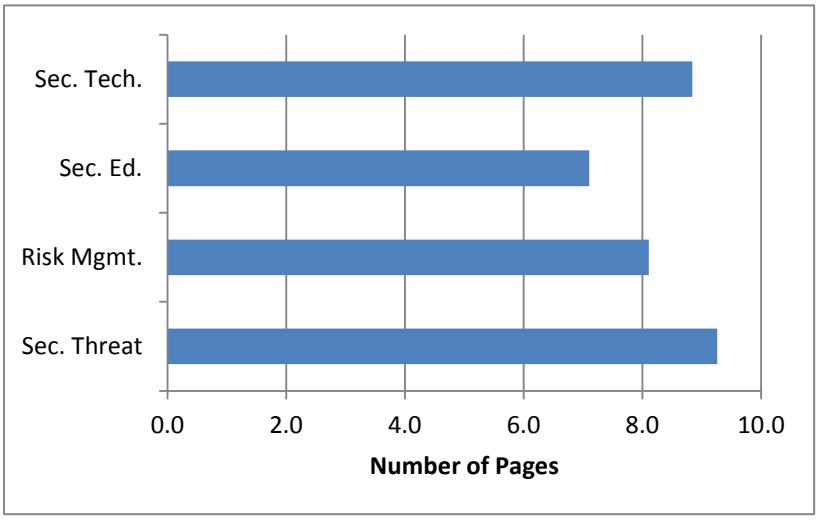


Figure 3 – Analysis of Page Count

content should also be measured by the magnitude of the content as defined by the page count of the index citation(s). While the inclusion of a concept is important, the relevance and level of content can provide additional insight into the importance of the topic. Figure 3 provides a summary of the page count analysis by content area. Three of the content areas were covered with more than eight pages of textbook coverage. The lagging content area, security education, resulted in a page count of 7.1.

The fourth component of this study assessed the strength of the material written in the textbook. All four perspectives (table of contents, index, page count and

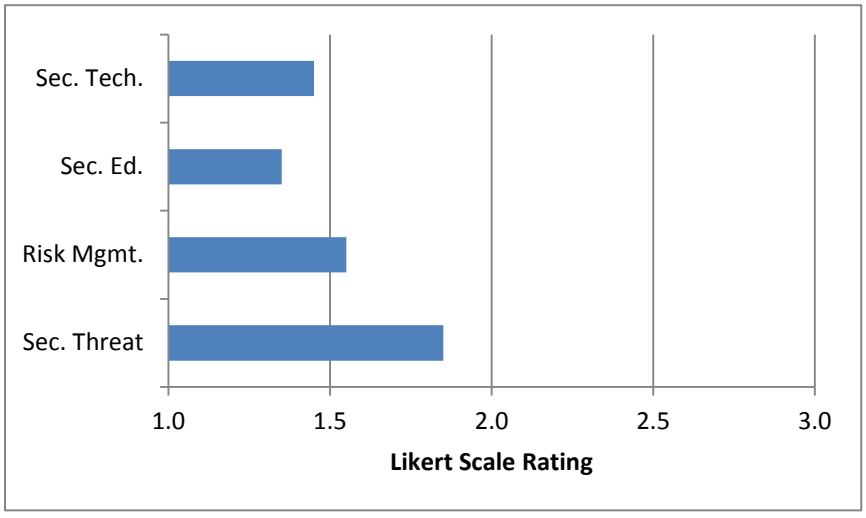


Figure 4 – Analysis of Content Quality

substance) can be used to develop an accurate and full evaluation of a content area. A five-point Likert scale was used to evaluate each of the content areas in the textbook

chapters. The results of the content evaluation, as shown in Figure 4, showed that each topic was rated at the lower scale of coverage (1 = minimal coverage). The security threat coverage area was rated the highest (1.9), but still at the lower value of the Likert scale.

Comparison of Results from Both Studies

This research study was a replication of a previous study completed in 2005. With the passage of seven years of technological, societal and industry usage, a comparison of the four assessments may gain some perspective on any changes to the inclusion of the content areas in the textbook population. After reviewing the analysis of the two studies, the topic of computer security has not been decreased over the last eight years.

The comparison of the table of contents shows a rather proportionate increase in coverage for all areas. As shown in Figure 5, the comparison of the two trend lines

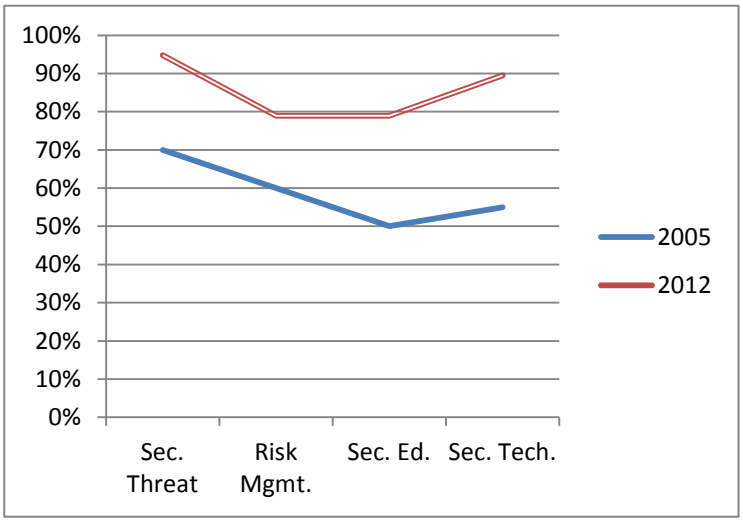


Figure 5 – TOC Analysis 2005 -- 2012

(for the research study years) illustrates a similar slope and direction to each of the lines. However, the gap between the two trend lines becomes more distant in the security education and security technology content areas. In 2012, there is a clear and significant increase in the TOC coverage from the previous research study. For example, percentage change associated with the coverage for the security education and security technology increased by 58% (50% -- 78.9%) and 63% (55% -- 89.5%) respectively while the security threat and risk management increased by only 35% and 32% respectively.

An analysis of the two research studies on the index analysis showed some apparent differences. As shown in Figure 6, the security threat and security education

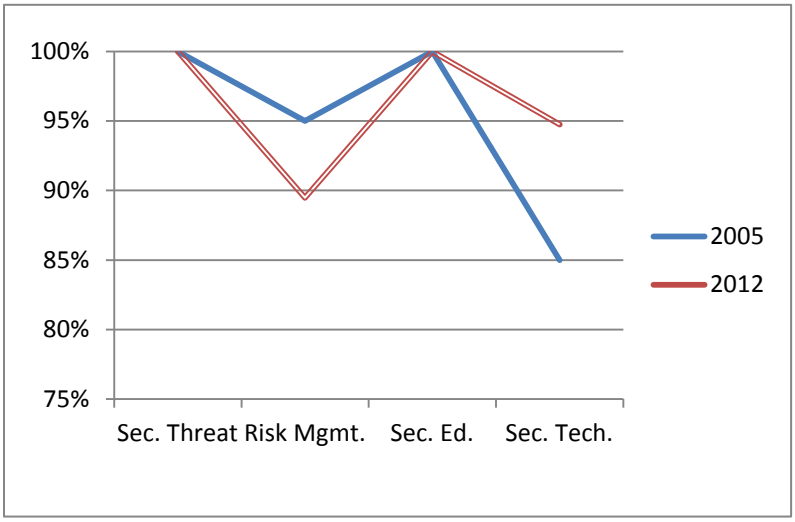


Figure 6 – Index Analysis (2005 – 2012)

content areas both maintained 100% coverage in each of the studies. However, the risk management and security technology content areas resulted in changes over the last eight years and in opposite directions. The results found that security technology increased by 10% in the most recent study while risk management declined about 6%.

The page count of the content areas has remained rather stable in two content areas when comparing the two research studies. As shown in Figure 7, the risk

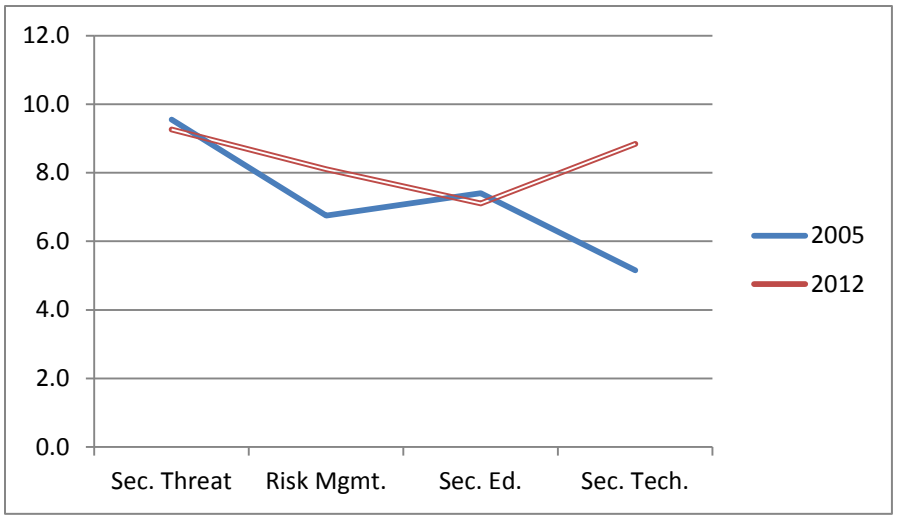


Figure 7 – Page Count Analysis (2005 – 2012)

management and security technology content areas changed; however, both increased in the latest study. Risk management resulted in a 1.3 page increase since 2005 while security technology increased by 3.6 pages; an increase of 20% and 72% respectively.

The quality of the coverage changed only slightly since 2005 for three content areas. The content associated with security technology increased significantly from 1.5

to 2.2 on the Likert scale; representing an increase of 49%. Risk management and security education increased at a smaller amount, 15% and 11% respectively.

CONCLUSION

Computer security will continue to be an important issue and its importance will become even more critical as business and society in general continually become more dependent on information technology and network interconnectivity. The frequency of citations in the tables of contents and indices of the textbooks that the researchers analyzed demonstrate that security issues continue to receive coverage in MIS textbooks. However, even though the research shows some improvement in coverage when comparing the two research studies in 2005 and 2012, additional attention by textbook publishers and authors is needed to provide more in-depth coverage of these important topics. In addition, professors need to supplement the textbook coverage with timely and updated information through electronic sources and articles.

Additionally, the researchers do not believe that the responsibility to augment textbook coverage is strictly an information systems department responsibility. An exposure and understanding of computer security is needed at all levels of an organization. Business activities are not viewed, processed or analyzed independently. Therefore, the secure processing, access and storage of organizational data can no longer be a single-source responsibility. Additionally, the nature of the threats relating to computer security evolves to correspond to the changes in technology and its adoption by business organizations. For example, the rapid adoption of smartphone technology by customers to complete business transactions has created an entirely new "venue" of security threats. Clearly, it is a significant challenge for authors and publishers to provide textbook materials that remains timely and current with the evolving security threats. It is important that faculty members, from all business disciplines, must develop methods to educate students on how to address computer security issues at various levels of the business enterprise.

The results of this research may act as a teaching aid for enhancing the coverage of security topics in all classes but especially in an introductory MIS course. A variety of sources are available, such as those shown in Table 2, which can be used to augment lectures and student projects. One example of a student assignment that has been used successfully by the researchers is the Briefing Paper. For this assignment, students select an article from the current literature and make a presentation to the class to discuss the salient points in the article. This assignment is an effective way to engage students to read and understand the current literature as it addresses computer security issues. Student teams could then be assigned to visit local businesses to gain perspective on the new knowledge on computer security issues. Ultimately, it is important to develop experiential assignments and opportunities for students to "personalize" how security will affect their future careers and personal lives.

The collection of web sites shown in Table 2 below provides the opportunity for a range of security topics to be examined. The contents of these sites can provide the instructor with the appropriate and timely content to select diverse and engaging

assignments for students. In addition, these resources can offer recent, additional material to supplement textbook content.

TABLE 2

COMPUTER SECURITY WEB SITES

Web Site	URL Address
CERT® Coordination Center	http://www.cert.org
The Internet Security Alliance	http://www.isalliance.org
Disaster Recovery	http://www.drj.com
ADDSecure.Net Inc.	http://www.addsecure.net
The Institute of Internal Auditors	http://www.theiia.org
Stanford Research Institute	http://www. sri.com
The SANS Institute	http://www.sans.org

- There are many security topics at the CERT® web site , but the site that should be of particular interest to students, as most own their own computer, relates to home network security. This web site has information on security, technology, risks to home users, accidents and other risks, and actions that can be taken to protect you home computer system.
- The Internet Security Alliance was created to provide a forum for information sharing and thought leadership on information security issues.
- The Disaster Recovery site is a fee-required site for certain archival information, but provides free access to its journal, the Disaster Recovery Journal. The Journal is dedicated to the field of disaster recovery in business, and was the first publication to do so. There are currently over 60,000 subscribers.
- The ADDSecure web site is a network security audit site. One of their main functions is to review the integrity of corporate networks and servers, including web and email servers. There is free access to its journal, The Journal of Internet Banking and Commerce. Topics covered in the journal include networks, Internet, and database, security, risk assessment and management, viruses, worms, and other malicious code, and mobile and satellite security.
- The Institute of Internal Auditors was formed in 1941. It serves as the global voice for the internal auditing profession. Its web site provides international standards for internal auditing as well as certification, research, and educational products, through its ITA Research Foundation.
- The Stanford Research Institute web site is an independent, nonprofit research institute that conducts research and development for business, government, foundations, and other types of organizations. Among its many activities are issues of security. Within that area it conducts risk forums, and computer security workshops. The information from its foundation workshops is available at no charge.

- The SANS Institute (SysAdmin, Audit, Network, Security) web site is the largest source of information security training in the World. It also develops, maintains, and makes available at no cost, the largest collection of research documents about various aspects of information security.

As stated in the introduction, students need to develop an awareness of computer security issues regardless of their major. Therefore, it is important to supplement the textbook coverage with assignments to learn and understand these issues. Some examples of assignments can ask students to explore security topics by visiting the following sites:

- CERT® Coordination Center site and prepare a report on security risks and prevention when installing a home computer.
- Internet Security Alliance site and prepare a report that analyzes and forms conclusion about a particular forum topic on computer security.
- Disaster Recovery site and prepare a report on terrorist's attacks and their potential effect on businesses.
- ADDSecure.Net Inc. site and prepare a report on e-commerce security issues.
- Institute of Internal Auditors site and prepare a report on internal auditing issues in Iraq.
- Stanford Research Institute site and prepare a report on risks to the public when using wireless systems.
- SANS Institute site and prepare a report on security training.

One additional site that the authors noted was on-line magazine http://www.scmagazine.com, which allows instructors to be up-to date on the latest news in the cyber world of security. Opportunities at this site include the option to receive a security newsletter, email and access to whitepapers on these security topics. Students could be given assignments from this information. Sites, such as this with a wealth of information, lead to other sources of reference material. Cyber security issues are too important to be ignored.

Obviously, there are numerous web sites that can be used when compiling security assignments, so many that we have provided an additional list in Appendix B. The links to these sites have been categorized by the four major areas of systems security covered in this paper. These additional sites provide significant and relevant material that can be used in conjunction with these assignments, with refinement by the instructors. The assignments can also be presented in class by students or can be synthesized by the instructor and then becomes part of a general class discussion, or any variation thereof. The point is that learning is now active, not passive.

The fast-paced changes in technology require similar changes to the delivery of academic instruction in technology-based courses. The integration of technology concepts, such as those described in this paper, must be supplemented by materials and assignments which will expand the limited coverage in the textbooks. The gap between the coverage of these topics and their importance can only be improved thought the integration of these assignments in a formal education environment. The

expanded knowledge gained will provide a positive element to students as a consumer and user of technology as well as a future business employee in a corporate organization.

APPENDIX A

Textbook Portfolio Listing

Applegate, Lynda M.; Robert D. Austin; Deborah L. Soule (2009). Corporate Information Strategy and Management". New York: McGraw-Hill Irwin

Baltzan, Paige (2012).Business Driven Information Systems. 3rd ed. New York: McGraw-Hill/Irwin.

Baltzan, Paige (2013). Information Systems. 2nd ed. New York: McGraw-Hill/Irwin.

Bidgoli, Hossein (2011). MIS. Boston, MA: Course Technology Cengage Learning.

Kroenke, David (2012). Using MIS. Upper Saddle River, NJ: Prentice Hall.

Kroenke, David and Earl H. McKinney, Jr. (2013).Process, Systems, and Information. Upper Saddle River, NJ: Prentice Hall.

Laudon, Ken, and Jane Laudon (2012). Management Information Systems. 12th ed. Pearson Prentice Hall.

O'Brien, James A and George M. Marakas (2011). Management Information Systems, 10th ed. New York: McGraw-Hill Irwin

Oja, Dan, and June Parsons (2013). Computer Concepts 2013. Boston, MA: Course Technology.

Oz, Effy. Management Information Systems (2009). Boston, MA: Thomson/Course Technology.

Pearlson, K. E., & Saunders, C. S. (2013). Managing & Using Information Systems (5th ed.). Hoboken, New Jersey: John Wiley & Sons Inc.

Rainer, R. Kelly and Casey G. Cegielski (2011). Introduction to Information Systems. Hoboken, NJ: John Wiley & Sons

Rainer, R. Kelly and Hugh Watson (2012). Management Information Systems Hoboken, NJ: John Wiley & Sons.

Stair, Ralph M., and George Walter Reynolds (2011). Fundamentals of Information Systems. 6th ed. Boston: Course Technology/Cengage Learning.

Stair, Ralph M., and George Walter Reynolds (2012). Principles of Information Systems. 10th ed. Boston: Course Technology, Cengage Learning.

Turban, Efraim, and Linda Volonino (2011). Information Technology for Management: Improving Performance in the Digital Economy. 8th ed. Hoboken, NJ: Wiley.

Valacich, Joseph S., and Christoph Schneider (2012). Information Systems Today: Managing in the Digital World. 5th ed. Boston: Prentice Hall.

Wallace, Patricia (2013). Information Systems in Organizations: People, Technology, and Processes. Boston: Pearson.

APPENDIX B

Additional Websites

Risk Management\2012 US asset management risk survey – Ernst & Young – Asset Management - Ernst & Young - United States.mht
http://www.ey.com/US/en/Industries/Financial-Services/Asset-Management/2012_US_asset_management_risk_survey

Risk Management\Financial industry lacks timely data to carry out risk management study.mht
http://www.thestreet.com/story/11731234/1/financial-industry-lacks-the-timely-data-needed-to-carry-out-in-depth-risk-management.html

Risk Management\NIST Risk Mgmt. Guide.pdf
http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

Risk Management\The Institute of Risk Management.mht
http://www.theirm.org/

The Seven Habits of Highly Effective Risk Managers Risk Management.mht
http://www.amanet.org/site-search-results.aspx?search_terms=7+habits&ibp-adgroup=habits&ibp-keyword=7+habits+of+highly+effective+people&ibp-matchtype={matchtype}&wm_crID=11874492&wm_lpID=63931937&wm_ctID=152&wm_kwID=31275524&wm_mtID=1&wm_content=0&wm_g_crID=11321778404&wm_g_kw=7+habits+of+highly+effective+people&wm_g_pcmt=&wm_g_cnt=0&gclid=CJyu7NyRtrUCFcef4Aod60gA3A&wm_kw=7+habits+of+highly+effective+people&wm_sd=1

Security Education\Center for Homeland Defense & Security Colleges and Universities Offering Homeland Security Programs.mht
http://www.chds.us/?special/info&pgm=partner

Security Education\DHS Education Programs.mht
http://www.dhs.gov/national-cyber-security-awareness-month

Security Education\NSEP - National Security Education Program.mht
http://www.nsep.gov/

Security Education\Security Education - Security Center - Cisco Systems.mht
http://tools.cisco.com/security/center/viewAlert.x?alertId=7197

Security Education\SETA Home.mht
http://www.comgt.com/security/SETA/

Security Technology\BBC - Future - Technology - How good is the latest personal security tech.mht
http://independentblogger.files.wordpress.com/2010/02/internet-privacy-and-security-best-practices-2010-05-181.pdf

Security Technology\Institute for Security, Technology, and Society.mht
http://www.ists.dartmouth.edu/

Security Technology\Security & Privacy - The latest security news - CNET News.mht
http://news.cnet.com/security/
http://www.securityinfowatch.com/magazine/stec

Security Technology\Technology News Security.mht
http://www.technewsworld.com/perl/section/security/

Security Threats\b-istr_main_report_2011_21239364.en-us.pdf
http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf

Security Threats\Congress Says Chinese Telecom a Security Threat Discovery News.mht
http://news.discovery.com/tech/apps/congressional-report-huawei-121008.htm

Security Threats\RSA Five Top Internet Security Threats in 2012.mht
http://www.notebookreview.com/default.asp?newsID=6310

Security Threats\Security Predictions 2012 & 2013 - The Emerging Security Threat.mht
http://www.sans.edu/research/security-laboratory/article/security-predict2011

Security Threats\SophosSecurityThreatReport2012.pdf
http://www.phoenixs.co.uk/phoenixblog/post/2012/03/20/Sophos-Security-Threat-Report-2012.aspx

REFERENCES

The Columbia Encyclopedia. Sixth ed: Columbia University Press, 2002. Print.

Anonymous. *2012 Cost of Cyber Crime Study: United States*. Traverse City, MI2012. Print.

---. "Congress Addressed on Cloud Computing Security, Opportunities and Risks." *International Journal of Micrographics & Optical Technology* 29.1 (2011): 4-5. Print.

---. "Develop a Computer Deployment Plan That Includes Security Issues." 2003. Web. 9/10/2003 2003.

---. "Gartner: Cloud Will Be Bulk of It Spending by 2016." *Information Management* 48.1 (2014): 7. Print.

---. "IBM Targets Cloud Computing with Security Infrastructure Services." *Informationweek - Online* (2010). Print.

---. "Introduction to Risk Analysis." 2003. Web. 9/10/2003 2003.

---. "ISO 177799 Directory." 2003. Web. 9/10/2003 2003.

---. "Likert Scaling." William M.K. Trochim 2004. Web. 1/19/04 2004.

---. "Occupational Outlook Handbook." Bureau of Labor Statistics 2012. Web. July 27, 2013 2013.

Au, Danelle. "The Weakest Link in Data Center Security." SecurityWeek.Com 2012. Web. February 1, 2013 2013.

Bachrach, K. S. "Interview. Via Email (Ed.)." 2003. Print.

Bednar, Joseph. "Hacking It." *BusinessWest* 30.3 (2013): 34. Print.

Chang, Kuo-Chung, and Chih-Ping Wang. "Information Systems Resources and Information Security." *Information Systems Frontiers* 13.4 (2011): 579-93. Print.

Chaudhary, Vikram. "Data Loss in a Virtual World." *Financial Express* 2013 Jun 17 2013. Print.

Cheng, Fred. "Security Attack Safe Mobile and Cloud-Based One-Time Password Tokens Using Rubbing Encryption Algorithm." *Mobile Networks and Applications* 16.3 (2011): 304-36. Print.

Erbschloe, Michael. *Guide to Disaster Recovery*. 1 ed. Boston, MA: Course Technology, 2003. Print.

Greenwald, Judy. "Putting Information in the Cloud." *Business Insurance* 48.4 (2014): 20-21. Print.

Holden, Greg. *Guide to Firewalls and Network Security: Intrusion Detection and Vpns*. Boston, MA: Course Technology, 2004. Print.

Kirk, Jeremy. "A Better Reason Not to Use Huawei Routers: Code from the 1990s." *InfoWorld.com* (2012). Web.

MacDonald, Laurie, and Kenneth Fougere. "Software Piracy: A Study of the Extent of Coverage in Introductory Mis Textbooks." *Journal of Information Systems Education* 13.4 (2003): 325-30. Print.

Mensch, Scott, and LeAnn Wilkie. "Information Security Activities of College Students: An Exploratory Study." *Academy of Information and Management Sciences Journal* 14.2 (2011): 91-116. Print.

Potter, Bruce. "Coming to Grips with Security." *IT Professional Magazine* 13.3 (2011): 14-17. Print.

Sousa, Kenneth J., Laurie E. MacDonald, and Kenneth T. Fougere. "Computer Security in the Introductory Business Information Systems Course: An Exploratory Study of Textbook Coverage." *Journal of Education for Business* 81.1 (2005): 15-20. Print.

Sposito, Sean. "In Wake of Data Breaches, Banks Face Huge Losses: Survey." *American Banker* 2013 Aug 08 2013. Print.
Vaquero, Luis M., Luis Rodero-merino, and Daniel Morán. "Locking the Sky: A Survey on Iaas Cloud Security." *Computing. Archives for Informatics and Numerical Computation* 91.1 (2011): 93-118. Print.
Volonino, Linda, and Stephen R. Robinson. *Principles and Practice of Information Security*. Boston, MA: Prentice Hall, 2004. Print.
Whitman, Michael E., and Herbert J. Mattford. *Principles of Information Security*. 1 ed. Boston, MA: Course Technology, 2004. Print.

Note: Title graphic by Carole E. Scott