THE JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 2 | Number 4 Article 3

2007

Making Molehills Out of Mountains: Bringing Security Research to the Classroom

Richard G. Taylor
University of Houston

Making Molehills Out of Mountains: Bringing Security Research to the Classroom[1]

Richard G. Taylor
University of Houston
rgtaylor@uh.edu

ABSTRACT

Security research published in academic journals rarely finds its way to the business community or into the classroom. Even though the research is of high quality, it is written in a manner that is difficult to read and to understand. This paper argues that one way to get this academic research into the business community is to incorporate it into security classrooms. To do so, however, academic articles need to be adapted into a classroom-friendly format. This paper suggests ways to do this and provides an example of an academic article that was adapted for use in a security management class.

Keywords: information security, pedagogy, academic research, teaching cases, research relevance

1. INTRODUCTION

> *"Does not the scientist have an obligation to publish? The standard answer is Yes. But does he not also have an obligation to be read? The standard answer…ought to be Yes, although…I sometimes think it is No. A man writes something…that is so dull that it is hard work to get through it: has he not missed his responsibility to the science? The egoistic savant thinks not; he thinks it is the reader's job to work hard so as to understand him."*
>
> Edwin G. Boring, Letter in *Contemporary Psychology*

Is there a place for academic research in the security curriculum? How many security educators read the academic journals in search of material to incorporate into their curriculum? My guess would be not many. Why is this? Does academic research have no applicability to security classroom teaching? This paper will look at these questions and provide suggestions to bring academic security research into the security classrooms.

Let's face it. Articles published in top-tiered academic venues are difficult, and (very) often un-enjoyable, to read. There, I said it! I realize that at any time now the academic gods may strike me down. The quality of this research

[1] This article was presented on September 28, 2007 at the InfoSecCD conference in Kennesaw, GA.

is of a very high standard, written by knowledgeable researchers, but the research is often underutilized because it never makes it way to a classroom (or directly to practitioners).

This is too bad. Security education needs a balance of theory and practice, however incorporating the two is not an easy task. Steven Alter (2001) explains that he has used many ideas taken from academic journal articles to incorporate in his MIS textbooks (Table 1).

Mintzberg	how managers use information
Simon	steps in decision making
Tversky, Kahneman, Slovic, et al.	common flaws in decision making
Markus	different views of user resistance
Hammer and Champy	reengineering examples
Standish Group	failure rates of information systems
Ives and Olsen	different levels of user involvement
Neumann	information systems risks
Mason	PAPA (privacy, accuracy, property, access) framework for ethical issues
Sviokla	how the implementation process affects success

Table 1. Academic Research incorporated Steven Alter's MIS textbooks. (Alter, 2001).

One of the primary reasons academic research is not included in classroom education is the belief that the research has little relevance to practice. A goal of classroom education is to teach material that will be useful to the students when they enter the business community. While reviewing many academic security articles, it seems like there are indeed some that would have little relevance to the classroom or to practice. However, many contain research that would benefit both students and practitioners. This relevant research needs to find its way into security classrooms.

2. RESEARCH RELEVANCE

A comment was posted on AISWorld that started a debate on the relevance of MIS research to the business community:

> *There are probably no academic findings of any importance in IT and few, if any, from business schools in general. The evidence is simply that few, if any, business people bother to waste their time with academic journals. Certainly, managers at Microsoft, Sun, Intel, etc. spend no time with academic findings. The important work is done by corporations, the government, or individuals in the pursuit of profit.*

The research published in top-tiered journals and conferences is very "academic" in nature, founded upon strong theory and meticulous methodologies. While the academic community views these publications to be the type of research that advances knowledge in the MIS discipline, the articles are often not "reader friendly", and would be very difficult, if not painful, for undergraduate (or graduate) students to read. Articles published in the top academic journals are difficult to read because of "(1) lifeless writing styles, (2) pretentious language, (3) unnecessary use of unfamiliar jargon, (4) numerous references to articles and books readers are unfamiliar with and can't easily obtain, and (5) extensive reliance on statistical analysis that is uninteresting and unconvincing to most practitioners and many academics[2]" (Bennis & O'Toole, 2005, p.6).

Not only are the articles difficult to read, but many argue that they are no longer relevant to the business community (Nevill & Wood-Harper, 2001). The target audience for these articles is no longer the practitioners. Academic research is intended to be read by other academics. Keen (1991) argues that this in itself defines the relevance of the research. Academic research is now more concerned with rigor than with relevance.

"The actual cause of today's crisis in management education is far broader in scope and can be traced to a dramatic shift in the culture of business schools. During the past several decades, many leading [business] schools have quietly adopted an inappropriate—and ultimately self-defeating—model of academic excellence. Instead of measuring themselves in terms of the competence of their graduates, or how well their faculties understand important drivers of business performance, they measure themselves almost solely by the rigor of their scientific research" (Bennis & O'Toole, 2005, p.98). Research now conducted in business schools is produced to add respectability to the scientific and academic underpinnings of the university.

The MIS community has struggled with the "rigor versus relevance" issue for some time. The first major MIS publication was MIS Quarterly (MISQ). MISQ originated through a shared vision between the University of Minnesota's Management Information Systems Research Center (MISRC) and the Society for Management Information Systems (SIM), which is a practitioner-based organization. All SIM members received MISQ.

In 1992, Blake Ives was editor of MISQ, and in his March editorial comments he notes that MIS research is straying and loosing its relevance factor to the business community. Even though research universities claimed to seek closer relations to the business community, their research efforts do not indicate these efforts. Universities are more concerned with rigor than with relevance. Ives states that "[f]aculty many times appear either unable or, as is more likely the

[2] My apology if this article contains any of these characteristics.

case, unwilling to frame their findings in such a way as to highlight managerial applicability" (Ives 1992 p. iii). Ives still championed the idea to bridge the gap between research and practice in MIS research.

Bob Zmud followed Blake Ives as the editor of MISQ. In his editorial comments in March 1995 (Zmud, 1995), he announced that SIM would no longer receive copies of MISQ so that MISQ "could redirect its direction toward the academic community and away from the practitioner community" (p.v). This marked the end of practitioner-directed research in MISQ. The "scientific research" now desired by MISQ definitely requires skill; however the skill no longer focused on time in the field to investigate actual problems that managers face. Instead more emphasis was placed on statistics and experimental design, as well as meticulous analysis of data.

Another factor contributing to the lack of practitioner relevance of academic research involves the reward structure for faculty members. The road to tenure does not go through practitioner-based research. Young faculty members understand this explicitly. The pressure to publish in top-tiered academic journals to meet tenure requirement has resulted in a lack of attention to research that might benefit practitioners and students alike. This research-based promotion has resulted in business schools "filled with individuals whose main professional aspiration is a career devoted to science" (Bennis & O'Toole, 2005, p.100). For example, an IS scholar who continually publishes rigorous scientific research in MISQ or other "A" journals is considered a star, while another who publishes relevant articles in practitioner-based publications risks being denied tenure.

3. SECURITY RESEARCH

The top-tiered MIS journals are (arguably): MISQ, Information Systems Research (ISR), and the Journal of Management Information Systems (JMIS) (Lowry et al. 2004). Recently the Journal of the Association of Information Systems (JAIS), an electronically published journal, has been included in the level of "A" journals by many top MIS research departments (e.g. University of Georgia, Georgia State, University of Texas, University of Houston). These journals have an acceptance rate of less than 10%.

Since 2000, twenty security-related articles have been published in the top-tiered journals mentioned above.3 Only six were published before 2000 (See Appendix A for a list of all security-related articles published in the top-tiered MIS journals). Since 2000, security-related academic articles also appear in other quality MIS journals: 11 in Journal of Information Systems; 8 in

[3] To determine the articles that I included as security-related, I searched the journals using keywords of "security" and "privacy". I then reviewed the abstracts of those articles to arrive at my determination. Other security-related articles may have been published in those journals but were not detected using my method.

European Journal of Information Systems; 6 in Journal of Strategic Information Systems; and 5 in Information Systems Journal. The MIS top academic conference (ICIS) has included a Security and Assurance track for the last few years. These articles are often considered top-tier publications since the acceptance rate is very low (i.e. the 2006 Security and Assurance track at ICIS accepted less than 10% of the articles submitted). There have been 26 security-related publications in the ICIS proceedings since 2000.

ACM ToISS	ACM Transactions of Information & Systems Security
CS	Computers & Security
IS	Information & Security
IMCS	Information Management & Computer Security
ISS	Information Systems Security
IT	Infosecurity Today
IJSN	International Journal of Security & Networks
IJICS	International Journal of Information & Computer Security
IJIS	International Journal of Information Security
IJISP	International Journal of Information Security & Privacy
JCS	Journal of Computing Security
JDFSL	Journal of Digital Forensics, Security & Law
JIPS	Journal of Information Privacy & Security
JISSec	Journal of Information Systems Security

Table 2. Academic journals dedicated to security research

There are also journals solely dedicated to publishing security-related articles (Table 2). These journals serve as a venue for various types of researchers. While some, such as the Journal of Information Systems Security (JISSec), publish academic research, others such as Computers and Security offers articles published by academics and practitioners alike. Many of the articles published in Computers and Security are already in a classroom-friendly format and would make excellent readings for students[4]. JISSec is one of the newer security-oriented journals dedicated to publishing high-level academic research. As they appear in the journal these articles are not classroom-friendly, however many may contain research that could be useful in a security classroom. (See Appendix B for a listing of all articles published in JISSec since its inception in 2005).

Security research published in the academic journals and conferences is high-quality research often with significant findings; however the articles are often lost in the black-hole of academia. Many may consider this type of research not relevant to the practitioner community or the classroom; however the research may indeed be relevant, but the delivery method may just be

[4] Other journals such as Communications of the Association of Information Systems (CAIS), Communications of the ACM, and MISQe(xecutive) publish classroom-friendly articles.

inappropriate, resulting in the articles being overlooked by security educators[5]. The goal here is to get the valuable research findings out of academic community and into the business community to have practical application. One of the best ways to do this is to incorporate the research into the classroom so future security professionals can apply the knowledge when they enter to work environment (Figure 1). Teaching the research findings in a classroom will eventually find its way to the practitioner community; however only 10% of academics felt that access to practice via student is important (Nevill & Wood-Harper, 2001).

Figure 1. Improving relevance of academic security research

Analyzing security-related research in top-tiered journals (Appendix A) produced some interesting articles with findings that could be useful in the classroom. Some of those articles include (but not limited to): *The Economic Incentives for Sharing Security Information* (Gal-or & Ghose, 2005); *The Value of Intrusion Detection Systems in Information Technology Security Architecture* (Cavusoglu et al., 2005); *Six Design Theories for IS Security Policies and Guidelines* (Siponen & Iivari, 2006); *Including Technical and Security Risks in the Development of Information Systems: A Programmatic Risk Management Model (Dillon, 2003); Coping With Systems Risk: Security Planning Models for Management (Straub & Welke, 1998)*[6].In their current format, students would find these articles difficult and un-enjoyable to read. The challenge for security educators is to translate this academic research into a format that can be used and enjoyed by students.

4. ADAPTING SECURITY RESEARCH FOR THE CLASSROOM

Typically, articles published in academic journals are between 10,000 and 15,000 words (though some can be much longer)[7]. Although academic articles vary in their exact format, they typically contain an array of required information (Table 3). This information is considered necessary for an article to be included in an academic journal (much at the insistences of reviewers and editors). The information in the different sections shows the progression of the research process the author used to reach his/her conclusions. Though necessary in academic publications, much of the information would not be

[5] As an academic researcher I choose to keep the faith that our research is indeed relevant to the business community.
[6] I have used an adapted version of the Straub and Welke article in a security class.
[7] These numbers were obtained by reviewing articles published in MISQ and ISR.

needed for use in a classroom environment. For example, the literature review, methodology, and statistical analysis would not be needed. What are needed are the problems/research questions and the findings.

Section	Description
Introduction	Defines and describes the problem and/or research questions to be researched and the need for such research
Literature review	Provides an illustrative account of the theory/theories that will be used to investigate the stated problem/research questions
Methodology	Describes the research method that the researcher will use to evaluate the problem/research questions and the reasons why that method is appropriate
Analysis	Provides the findings obtained from the methodology that was utilized
Discussion	Discusses the findings
Conclusion	Provides a brief review of the intent of the paper and summarizes the findings and contributions. Also points out limitations to the research and suggests areas for future research.
References	List the references used to write the article

Table 3. The anatomy of an academic research article

Alter (2001) recommended that a short version and a long version be created for each academic article. The shorter version would be developed to demonstrate relevance for the classroom and for practitioners, while the longer versions would demonstrate academic rigor and include more in-depth discussions of theories, methodologies, and statistical analyses. However, authors have little incentive to create an alternative version of their article for classroom use. The tenure process sees to that.

The shorter classroom-friendly versions of research articles could take the form of research reports, technology briefings, or case studies. Research weighted with heavy statistical analyses may be more difficult to translate to a classroom environment, while case studies may be more easily adapted. A great deal of security research is written using the case study method. Articles that do not use the case study method should not be rejected as classroom material. These articles still have the required components: a problem/research question and the findings. With these components, a creative educator can develop useful

material to be used as teaching aids for security students. One such teaching aide is the security case study.

5. SECURITY CASE STUDIES

Case studies allow students to simulate real-world situations. For this reason, they are widely used in management courses. Case studies typically involve working in a team environment, allowing students to use problem solving skills to attack problems from different perspectives (Sirias, 2002). Case studies allow educators to "use narrative and stories to allow students to enter the culture, help them progress from the role of listener to active participant, and engage in problem solving in the stories that mimic real life settings" (Hsu & Backhouse, 2002, p. 212). This can improve students desire to learn and can often be more affective that classroom lectures.

Creating security case studies from academic articles will allow for the replacement of abstract concepts with stories that help the students see a problem and give them the opportunity to come up with their own solution. By incorporating the research findings into the case study, students will be able to discuss how these findings can be applied to real world security situations. Security educators should encourage students to make recommendations and provide solutions to the issues or problems presented in the case, based on the knowledge that the students acquire in the class (Sirias, 2002). Security case studies can allow students to gain knowledge about information security and its impact on the business environment.

Writing teaching case studies is significantly different from writing academic research articles. Case studies should tell a story to engage the reader. Good storytelling abilities improves the effectiveness of a teaching case. There are eight elements that should be included in a security teaching case (adapted from Cappel & Schwager 2002):

1. ***Addresses security subject matter for a specific security problem or course***. A case study that may be appropriate for a security management class may not be useful in a cryptography class, or vice versa.
2. ***Has a clear purpose***. The case should contain a clear theme or message, and address the type of knowledge or mental process that the students should utilize.
3. ***Provides realism***. The students should feel like the problems are from a real business situation. This adds to their feeling of accomplishment when they address potential solutions.

4. ***Is of appropriate length***. A case should be long enough for the student to clearly understand the situation and give them the opportunity to address the issues presented.
5. ***Is objective in presentation and tone***. The case should be as neutral as possible, without containing any of the writer's opinions. This allows the students to develop their own solutions without the pressure to agree with the writer.
6. ***Has a hook***. There should be a statement or short paragraph at the beginning that grabs the readers' attention. This hook could be included in an abstract.
7. ***Addresses a timely topic***. The case should involve recent security topics.
8. ***Has been pre-tested***. Have other colleagues look over the case before use.

Discussion question can be included at the end of the case for students to use, or can be included in teaching notes. Discussion questions should guide the students in "applying theories or concepts to situations, distinguishing relevant from irrelevant facts, evaluating actions, looking at problems from multiple vantage points, and developing alternatives and solutions" (Cappel & Schwager 2002, p. 288).

Below is an example of how an academic research article was reformatted into a teaching case study to be used in a classroom environment.

6. A TEACHING CASE EXAMPLE

As an example, I will discuss how an article published in the 2006 ICIS proceedings—***Management Perception of Unintentional Information Security Risks*** (Taylor, 2006)—was converted to a teaching case study. Because it was published in a top-tiered academic venue, it was highly unlikely that it will ever be read by practitioners, or incorporated into a security class. However, the case study did result in some interesting findings that could be beneficial to practitioners and students alike. Therefore, the article could be included in a security class if it were rewritten and formatted in a way that would be "classroom friendly".

The case deals with security management issues, focusing on the human aspect of information security[8]. The study deals with an area of information security that has received little attention: unintentional security risks. These risks include any action by an employee that unintentionally put the organization's information at risk. These actions could include sharing system passwords,

[8] The case study narrative in this article was already written in a reader-friendly manner, so it was easily converted to a teaching case.

leaving sensitive information unsecured on desks or in unlocked file cabinets, and/or throwing sensitive information in the trash. The case study was conducted in a financial institution and includes comments from key personnel, including the CEO, CIO, other executives and managers, IT employees, and support staff[9]. The case study also includes observation made by the author regarding the level of security of the organization. Three findings came out of the original study:

1. Management perceives the level of information security within their organization to be high.
2. Management perceives that employees adhere to established information security policies.
3. Management is unaware of employees' actions that may unintentionally expose organizational information to security risks.

The original paper was 16 pages in length with approximately 11,000 words. This would be too long to use in a classroom. By eliminating the literature review and methodology sections, the paper was almost cut in half, resulting in a more manageable case. Further reduction improved readability, ultimately arriving at a classroom-friendly case study of approximately 6 pages. Note that even though over half the paper was eliminated, the key components still remain: the problem and the findings.

Reducing the case study to a manageable size and improving the readability added to the classroom friendliness. However, more was needed before the case study was ready to be introduced to a security class. A section was added that enticed the students to think about the case, and to discuss the specific situation. Discussion questions added to the end of the reformatted article helped facilitate this. While this case describes a specific situation, its focus was not to provide a solution to the problems identified. This leaves an opening for students to discuss how management can change their perception and raise their awareness of these unintentional security risks. These changes that were made to this academic paper made it appropriate, and even beneficial, for use in a security management class.

Discussion questions were added to the case study (Table 4). The questions were added at the end of the case study to allow the students a chance to review the case and develop their own answers. The students were then put in teams to discuss the questions. Finally, the case was discussed in class with each team sharing their thoughts and opinions.

[9] In the case study, I made up names to use in place of the organizational position. This contributed to the realism of the study.

Discussion Questions
1. Discuss the difference between intentional and unintentional information security threats. 2. Explain the significance of unintentional threats in organizational security. Are these threats a real problem for organizations? 3. Why do employees do these actions that unintentionally put the organization's information at risk? 4. How can employees be motivated to stop? 5. Does management take these threats seriously? 6. How can managers alter their perceptions of these types of threats? 7. If management's perceptions are not altered, what will be the affect on the organization? 8. Are there technology-based security solutions that can help reduce these threats? 9. Who in the organization is responsible for addressing these types of threats? Is this an IT problem? 10. What should managers do to eliminate or reduce these threats? 11. Can these threats be eliminated?

Table 4. Case study discussion questions

This is only one example of using academic research that is often considered irrelevant to business practice. The same could be accomplished by adapting other academic publications. Some articles may not lend themselves to an easy adaptation; however many will provide enough information to at least create a mini-case study of one or two pages. These mini-cases are much more focused on a single concept and can be discussed in a short time (Sirias, 2002).

When you find an article that you would like to adapt for classroom use, attempt to work with the original author if possible. If not be sure to give credit to the author for his/her research efforts. Once case studies (or other work created for the classroom) are created, they can be posted in a venue where other security educators can access and use.

Here are some guidelines to follow.

1. Stay current with academic security research
2. Identify research that is relevant for classroom use

3. Reformat the research to be appropriate for classroom (i.e. case study, technology briefing, or just an abbreviated version)[10]

4. Introduce the classroom-friendly research to your students

Be aware that by reading journals you may come across articles that are classroom-friendly as published (with some needing only minor adaptations). Some examples are: *Anything You Say Can Be Used Against You in a Court of Law: Data Mining in Search Archives (Ives & Krotov, 2006), Understanding Disaster Recovery Planning through a Theater Metaphor: Rehearsing for a show that might not open (Kendall et al., 2005), Future Security Approaches in Biometrics (Boukhonine et al., 2005), What is a Chief Privacy Officer? An Analysis Based on Mintzberg's Taxonomy of Managerial Roles (Kayworth et al., 2005), Computer Crime at CEFORMA: a case study (Dhillon et al., 2004), Computer Crime: theorizing about the enemy within (Dhillon & Moores, 2001), Violations of safeguards by trusted personnel and industry related information security concerns (Dhillon, 2001), Recovering IT in a Disaster: Lessons from Hurricane Katrina (Junglas & Ives, 2007).*

Many security educators may have abandoned journals for useful classroom material. Though there is always the Harvard Business Review and the Sloan Management Review that provides excellent teaching cases, don't give up on other journals. Be on the lookout for hidden gems that require little, or no, modifications. These can add a valuable dimension to the learning process of your students.

7. CONCLUSION

This paper is not insinuating that security research in academic publications is unnecessary or irrelevant, just that the research as it is presented for publication is typically not classroom-friendly. There seems to be no relief on the horizon. Scientific research will continue in MIS, including research on information security. Therefore if this research is to be incorporated into the classroom, it will take a proactive approach from those who are dedicated to teaching information security. The inclusion of this research into the classroom will help establish a balance between theory and practice for students.

Not all academic research papers will be adaptable for classroom use; however for those that can, there are benefits to bringing this research to the classroom. The bottom line is this: good security research is being published by knowledgeable authors, yet the research is not finding its way to practitioners or to the classroom. With a little effort, this research can be brought to the

[10] Universities that have access to PhD (or other graduate) students can use that resource to create classroom-friendly material from academic research.

classroom and ultimately make its way to the business community. It is the security educators' task to make classroom molehills out of academic research mountains.

REFERENCES

Alter, S. (2001). "Recognizing the Relevance of IS Research and Broadening the Appeal and Applicability of Future Publications." Communications of the Association for Information Systems, 6(3): 1-9.

Bennis, W. G. and O'Toole, J. (2005). "How Business Schools Lost Their Way." Harvard Business Review March: 96-104.

Boukhonine, S., Krotov V., and Rupert, B. (2005). "Future Security Approaches to Biometrics." Communications of the Association for Information Systems, 16(48).

Cappel, J. J. and Schwager, P.H. (2002). "Writing IS Teaching Cases: Guidelines for JISE Submissions." Journal of Information Systems Education, 13(4): 287-293.

Cavusoglu, H., Mishra, B., Raghunathan, S. (2005). "The Value of Intrusion Detection Systems in Information Technology Security Architecture." Information Systems Research, 16(1): 28-46.

Dhillon, G. (2001). "Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns." Computers & Security, 20(2): 165-172.

Dhillon, G. and Moores, S. (2001). "Computer crimes: theorizing about the enemy within." Computers & Security, 20(8): 715-723.

Dhillon, G., Silva, L., and Backhouse, J. (2004). "Computer Crime at CERORMA: a case study." International Journal of Information Management, 24(6).

Dillon, R. L. (2003). "Including Technical and Security Risks in the Development of Information Systems: A Pragmatic Risk Management Model." Proceedings of the 24th International Conference on Information Systems, Seattle, WA.

Gal-Or, E. and Ghose, A. (2005). "The Economic Incentives for Sharing Security Information." Information Systems Research, 16(2): 186-208.

Hsu, C. and Backhouse, J. (2002). "Information Systems Security Education: Redressing the Balance of Theory and Practice." Journal of Information Systems Education, 13(3): 211-218.

Ives, B. and Krotov, V. (2006). "Anything You Say Can Be Used Against You in a Court of Law: Data Mining in Search Archives." Communications of the Association for Information Systems, 19(29).

Junglas, I. and Ives, B. (2007). "Recovering IT in a Disaster: Lessons from Hurricane Katrina." MISQ Executive, 6(1).

Kayworth, T., Brocato, L. Whitten, D. (2005). "What is a Chief Privacy Officer? An analysis based on Mintzberg's Taxonomy of Managerial Roles." Communications of the Association for Information Systems, 16(6).

Keen, P. (1991). "Relevance and Rigor in IS Research: Improving Quality, Confidence, Cohesion and Impact", in Information Systems Research: Contemporary Approaches and Emergent Traditions, eds. H. E. Nissen, H. K. Klein and R. Hirshheim. Amsterdam, Elsevier Science, IFIP.

Kendall, K. E., Kendall, J.E., Lee, K. (2005). "Understanding Disaster Recovery Planning through a Theater Metaphor: Rehearsing for a show that might not open." Communications of the Association for Information Systems, 16(51).

Nevill, N. and Wood-Harper, T. (2001). "Choice of Target Audience for IS Research: Reflections on Discussions with IS Academic Leaders in the UK." Communications of the Association for Information Systems**,** 54(4): 1-37.

Siponen, M. and Iivari, J. (2006). "Six Design Theories for IS Security Policies and Guidelines." Journal of the Association for Information Systems**,** 7(7): 445-472.

Sirias, D. (2002). "Writing MIS Mini-Cases To Enhance Cooperative Learning: A Theory of Constraints Approach." Journal of Information Systems Education, 13(4): 351-356.

Straub, D. and Welke, R. (1998). "Coping With Systems Risk: Security Planning Models for Management Decision Making." MIS Quarterly, 22(4): 441-469.

Taylor, R. G. (2006). "Management Perception of Unintentional Information Security Risks." Twenty-seventh International Conference on Information Systems, Milwaukee, WI.

Appendix A: Security Research in Top-Tiered Academic Journals

Journal	Year	Article
MISQ	2007	The Value of Privacy Assurance: An Exploratory Field Experiment
	2007	Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal—Agent Perspective
	2006	Circuits of Poser in Creating De Jure Standards: Shaping an International Information Systems Security Standard
	2006	The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization
	1998	Coping With Systems Risk: Security Planning Models for Management
ISR	2007	Releasing Individually Identifiable Microdata with Privacy Protection Against Stochastic Threat: An Application to Health Information
	2006	Privacy Protection in Data Mining: A Perturbation Approach for Categorical Data
	2006	An Extended Privacy Calculus Model for E-Commerce Transactions
	2005	Maximizing Accuracy of Shared Databases with Concealing Sensitive Patterns
	2005	The Economic Incentives for Sharing Security Information
	2005	The Value of Intrusion Detection Systems in Information Technology Security Architecture
	1999	Morality and Computers: Attitudes and Differences in Moral Judgments
	1990	Effective IS Security: An Empirical Study
JMIS	2007	Interoperability of E-Government Information Systems: Issues of Identification and Data Sharing
	2006	An Information Systems Security Risk Assessment Model Under the Dempster-Shafer Theory of Belief Functions
	2006	Moderating Effects of Task Type on Wireless Technology Acceptance
	2000	Managing the Costs of Informational Privacy; Pure Bundling as a Strategy in Individual Health Insurance Market
	1999	Password Security: An Empirical Study
	1997	Preventive and Deterrent Controls for Software Piracy
	1989	Security of Statistical Databases with an Output Perturbation Technique
	1987	Improvements in Database Concurrency Control with Locking
JAIS	2006	A Design Theory for Securing Information Systems Design Methods
	2006	Six Design Theories for IS Security Policies and Guidelines
	2006	Concern for Information Privacy and Online Consumer Purchasing
	2006	Private Transactions in Public Places: An Exploration of the Impact of the computer Environment on Public Transactional Web Site Use
	2005	Theoretical Explanations for Firms: Information Privacy Behaviors
	2000	Illegal, Inappropriate, and Unethical Behavior in an Information Technology Context: A Study to Explain Influences

Appendix B: Journal of Information Systems Security (JISSec)

Journal	Year	Article
Vol. 1(1)	2005	Systemic Risk Redefining Digital Security
	2005	Information Warfare: A Comparative Framework for Business Information Security
	2005	The Ephemerizer: Making Data Disappear
Vol. 1(2)	2005	Methodology to Assess the Impact of Investment in Security Tools and Products
	2005	SoapSy – Unifying Security Data from Various Heterogeneous Distributed Systems Into a Single Database Architecture
	2005	Case Study: The case of a Computer Hack
Vol. 1(3)	2005	RFID: A Systematic Analysis of Privacy Threats & A 7-Point Plan to Address Them
	2005	WIDS – A Wireless Intrusion Detection System for Detecting Man-in-the-Middle Attacks
	2005	Botnets: The Anatomy of a Case
Vol. 2(1)	2006	Security Consistency in Information Ecosystems: Structuring the Risk Environment on the Internet
	2006	Security Issues and Capabilities of Mobile Brokerage Services and Infrastructures
	2006	A Conceptual Model for Integrative Information Systems Security
Vol. 2(2)	2006	Rating Certificate Authorities: A Market6 Approach to the Lemons Problem
	2006	Towards a Global Framework for Corporate and Enterprise Digital Policy Management
	2006	Managing Information Security: Demystifying the Audit Process for Security Officers
	2006	To Opt-In, or To Opt-Out: That is the Question: A Cast Study
Vol.2(3)	2006	Anchoring Information Security governance Research: Sociological Groundings and Future Directions
	2006	Building User Authentication in an Inter-Organizational Information System
	2006	How Secure is Your Password: An Analysis of E-Commerce Passwords and their Crack Times
Vol. 3(1)	2007	Ethics and morality – A Business Opportunity for the Amoral?
	2007	An evaluation of size-based traffic feature for intrusion detection
	2007	The effect of span and privacy concerns on e-mail user's behavior