Improving Information Security Risk Analysis Practices for Small- and Medium-Sized Enterprises: A Research Agenda

John Beachboard, Alma Cole, Mike Mellor, Steven Hernandez, and Kregg Aytes
Idaho State University, Pocatello, Idaho USA

beach@isu.edu alma@almacole.com michael@mellorsecurity.com
hernstev@gmail.com aytekreg@isu.edu

Nelson Massad
Florida Atlantic University, Florida USA

nmassd@fau.edu

Abstract

Despite the availability of numerous methods and publications concerning the proper conduct of information security risk analyses, small and medium sized enterprises (SMEs) face serious organizational challenges managing the deployment and use of these tools and methods to assist them in selecting and implementing security safeguards to prevent IS security compromises. This paper builds a case for and then outlines a possible approach and a multi-faceted research agenda for developing an "open development" strategy to address recognized deficiencies in the area of risk analysis to include developing: a multi-level risk assessment methodology and set of decision heuristics designed to minimize the intellectual effort required to conduct SME infrastructure level risk assessments, a set of decision heuristics to assist in the quantification of organizational costs, financial as well as non-financial, a knowledge base of probability estimates associated with specified classes of threats for use in the application of the aforementioned methodology and automated tool(s) capable of supporting the execution of the aforementioned methodology and heuristics.

Keywords: information security, information assurance, risk management, risk assessment, open source, open content

Introduction

It is commonly accepted that IT security countermeasures are imperfect thus organizations must be prepared to manage risk rather than attempt to eliminate it (Alberts & Dorofee, 2002; McCumber, 2005; Peltier, 2005; Schneier, 2004; Whitman & Mattord, 2003). A key element of the risk management process is the conduct of threat assessments and risk analyses that are tuned to the specific needs of the organization. The conduct of risk assessment and analysis is widely viewed as a necessary activity to guide the design and implementation of enterprise information security programs. The underlying framework for conducting such analyses is relatively simple. Identify and prioritize assets to be protected; identify relevant threats and the probability of their occurrence; multiply; add; then compare the expected losses with the costs of implementing relevant countermeasures. Of course, such analyses can be performed qualitatively, but the underlying logic remains largely the same.

The difficulties in effectively conducting such analyses are numerous. Identifying *all* relevant threats and *reliably* estimating the probability of occurrences have proven to be extremely difficult if not impossible. Likewise, estimating costs, even qualitatively, associated with various types of system failures or compromises is an inexact process. While the models for performing risk analyses are not difficult to understand, appropriately applying the models in given organizational contexts represents a daunting task. This is particularly true for resource- and expertise-constrained small- and medium-sized enterprises (SME). In the U.S., the term is more typically applied to small- medium-sized businesses having less than 500 employees; the term SME is more typically used within the EU to refer to firms with less than 250 employees (Storey, 2003). Either definition works for the purposes of this paper. Under either definition, these organizations are unlikely to include large IT staffs with dedicated or extensive information security expertise. As Jaquith (2007) notes, the information security world has widely adopted the paradigm of calculating annualized cost expectancies (ALEs), but, “there is just one problem with ALE: the old dog will not hunt….the numbers are too poor even to lie with” (p. 32). Jaquith cites three primary reasons for this (p.33):

- The inherent difficulty in modeling outliers.
- The lack of data for estimating probabilities of occurrence or loss expectancies
- Sensitivity of the ALE model to small changes in assumptions.

There are numerous commercial enterprises providing software tools designed to assist with this effort. Some of them, RiskWatch ® for example, claim to provide strong support for calculating annualized loss expectancy (ALE) and return on security investment (ROSI) (*RiskWatch*, 2005). While these tools may be quite effective, their use presents several practical issues for SMEs. First, they tend to be fairly expensive, although prices can vary significantly depending upon the features and support included. Second, they tend to be quite complicated. Effective use requires a significant amount of personnel training or consultant assistance as well as a significant amount of effort. Finally, for data quality problems referenced above, users have no real means of making an *a priori* evaluation of the quality of the final output.

Understandably, commercial companies prefer not to release their proprietary models and the knowledge bases employed in their products. However, without such information little opportunity exists for the user community to evaluate the relative efficacy of various products. Users are often permitted to download trial packages to evaluate the look and feel of program execution and reports but again lack an objective means for evaluating output quality.

To address these issues, this paper proposes the Information Assurance (IA) community adopt an “open source” approach to develop the following:

- A multi-level risk assessment methodology and set of decision heuristics designed to minimize the intellectual effort required to conduct SME infrastructure level risk assessments
- A set of decision heuristics to assist in the quantification of organizational costs, financial as well as non-financial

- A knowledge base of probability estimates associated with specified classes of threats for use in the application of the aforementioned methodology
- Automated tool(s) capable of supporting the execution of the aforementioned methodology and heuristics

At least initially, such an effort would be designed to meet the needs of profit and not-for-profit SMEs due to financial, time and intellectual constraints commonly associated with small organizations ("OCTAVE methods," 2003).

We recognize that this proposal is not necessarily unique. A search of Sourceforge.net, "the largest repository of Open Source code and applications available on the Internet" ("Sourceforge.net FAQ," 2006), revealed two risk assessment related projects. One project, CORAS, represents a European Union (EU) funded effort to develop software supporting model-based risk assessment for use in improving security during the systems design process. As such, the focus of CORAS is different than what we propose below. A second project, OpenSource Management of Risk (OSMR), is intended to provide a model-based risk analysis tool based on the ISO 17799 standard and is more in tune with the objectives of our proposal. However, the Sourceforge site reflects no evident progress on this effort and our attempt to contact the project director was unsuccessful. Additionally, the Computer Security Resource Center (CRSC) of the National Institute of Standards and Technology (NIST) provides Automated Security Self Evaluation Tool (ASSET) tailored to meet the needs of federal agencies seeking to comply with the *Federal Information Security Management act of 2002*, the Office of Management and Budget circular A-130 appendix III). (This tool is available for download at: http://csrc.ncsl.nist.gov/asset/ although this tool is no longer being supported by NIST.)

We also acknowledge the work accomplished by the Carnegie Mellon Software Engineering Institute in developing Operationally Critical Threat, Asset, and Vulnerability Evaluation^{sm} (OCTAVE^{sm}) and OCTAVE-S methods. OCTAVE-S is specifically designed to meet the risk analysis needs of smaller organizations (Harper, 2002). The guidance published for the OCTAVE-S method, developed specifically for small organizations, includes approximately 100 pages of guidelines and 400 pages of forms (available at: http://www.cert.org/octave-s/download). While we offer no objection or critique of the method *per se*, we remain concerned that the application of the OCTAVE-S's method will remain relatively limited due to the financial and cognitive constraints discussed above. There are numerous other analysis methods available for adoption, e.g., Facilitated Risk Analysis Assessment Process (FRAAP) (Peltier, 2005) or the risk management guidance published by NIST (National Institute of Standards and Technology, 2002). However, to varying degrees, all of these approaches entail levels of complexity and uncertainty that act as barriers to their effective adoption and application by SMEs.

The primary objective of the suggested program is to reduce the cognitive and financial burdens associated with conducting reasonably high quality risk assessments, thus promoting more extensive use of this critical risk management practice by SMEs. The fundamental assumption underlying our proposal is that the adoption of an open development approach can result in improved methodologies by fostering broad participation in the development of simplified risk models and the collection of risk data that can be used to populate those models. Furthermore, we believe that an open content approach can result in the production and dissemination of higher quality risk management data by exposing the methods and assumptions under which such data have been produced.

This paper provides a descriptive overview and supporting rationale for pursuing the four initiatives introduced above. The authors offer the following description and rationale as a "strawman" proposal for use in beginning a conversation among interested researchers and practitioners.

While recognizing that the implementation of the proposal identified above could evolve in many different manners, the balance of this paper describes a possible strategy as a means of gauging what level of interest might exist.

What Might Open Source Risk Analysis Look Like?

Utilizing the logic of structured decomposition associated with top-down systems analysis, a top level model could be populated with information gained from a short questionnaire, as exemplified below. Such a model could provide estimates of annualized loss expectancies for SMEs.

1. What is your organization's estimated annual revenue or budget?
2. Rate your organization's dependence upon IT to accomplish its mission.
3. Rate your organization's dependence on internet access to its mission.
4. Rate your organization's staff and management knowledge or expertise with respect to information security awareness/training.
5. Rate the effectiveness of your organization's technical security countermeasures.
6. Rate the effectiveness of your organization's management controls, information security policy and procedures.
7. Does your organization have verified data backup procedures?
8. Does your organization have a verified business or disaster recovery plan?
9. Does your organization have verified incident response capability?

We believe that it might be possible to input the answers to such questions into a model capable of making a rough calculation of information assurance risks associated with its current practices. Of course, the key to producing a useful estimate is the availability of reasonably good risk estimates and means for calculating the financial costs associated with various types of system failure. Techniques to produce such estimates are discussed in following sections.

We do not propose that the performance of such a calculation constitutes an acceptable risk analysis. However, we do see such a simplified model as serving as an effective introduction to risk management and analysis for SME management. We can envision multiple levels of drill-down or decomposition, the bottom layer reaching a level of rigor associated with established risk assessment models (e.g., OCTAVE-S, FRAAP, etc.). The idea is to reduce the cognitive and financial barriers of instigating a risk management process.

Accordingly, the following initiatives are designed to maximally benefit those organizations unable or unwilling to adopt existing "best practices" within this domain.

Initiative 1. Develop a Multi-level IA Risk Analysis Methodology and Decision Heuristics

Consistent with our understanding of the research approach advocated by Herbert Simon, we view the development of risk analysis methodologies as essentially consisting of the creation of simulation models (Simon, 1996). Simon argued that the use of simulations could be genuinely productive in the creation of knowledge about poorly understood systems. Dutta and Roy (2003) have demonstrated the use of simulation as a means of understanding organizational behavior relating to security management. While their model differs in scope and purpose from what we propose here, their work does demonstrate the methodological viability of such an approach as well as provide useful insights that might be adopted into initial modeling conducted in support of this initiative.

The development of a multi-level risk analysis methodology is meant to acknowledge the existing work that has been done in creating risk analysis models. To the extent that such models are available in the public domain (e.g., OCTAVE and CCTA Risk Analysis and Management Method (CRAMM)) we would rather adopt, adapt and extend such models than develop new models from scratch. The fundamental objective of this initiative is to achieve a higher level of abstraction that significantly simplifies the model's use while minimizing to the extent possible compromises in the quality of analysis.

Existing methodologies call for the comprehensive identification of threats (see for example, Schneier's discussion of attack trees (2004, pp. 318-333). Developing comprehensive lists associated with natural- and man-made disasters and the diverse and ever-expanding list of technical and behavioral exploits can prove to be an insurmountable task and one highly dependent upon the knowledge and thoroughness of the analyst. We suggest that it might be possible to usefully aggregate threats into threat classes, dramatically reducing the workload of the analyst without fully eliminating the granularity of information required for organizations to make investment regarding the selection of appropriate countermeasures. Whitman has proposed a very similar approach, identifying and prioritizing 12 threat categories according to weightings derived from an online survey of IT professionals (Whitman, 2003; Whitman & Mattord, 2003). Our intent would be to build on this fundamental work by greatly increasing participation in refining threat categories if required, and investigating whether vulnerability and exposure data can be usefully aggregated for application in a more abstract risk analysis model suggested above.

The end objective is to reduce the number of variables to be incorporated into the model. We anticipate the argument by experts that such abstraction could well undermine the integrity of the entire analysis process, thus producing meaningless results. We offer two responses. One, for reasons further articulated below, we are not entirely confident with the results obtained from expert consultants and commercial products. Second, with use and public scrutiny, model efficacy can be empirically assessed over time.

Initiative 2. Develop Decision Heuristics for Quantification of Organizational Costs

While we have not conducted formal research on the subject, the first author has missed few opportunities to query practicing accountants regarding methods used to estimate costs associated with specific types of security incidents. For example, when asked about how his company would assess the cost of lost productivity of back office staff due to a virus infection, an accountant specifically charged with the responsibility for IT investment analysis could offer no answer. His shrugged shoulders were not a unique response to this question.

Yet as evidenced by survey results from the FBI (Gordon, Martin, Lucyshyn, & Richardson, 2005) and CERT Coordination Center of the Carnegie Mellon Software Engineering Institute ("2005 E-crime watch survey," 2005), some companies will offer a quantitative response when asked. The FBI reported per respondent annual losses decreased from $141,496,560 in 2004 to $130,104,542 in 2005 – "for the 630 respondents that were willing and able to estimate losses…" (Gordon et al., 2005, p. 14). 47% of respondents in the CERT survey "could not say how monetary losses change from year to year" ("2005 E-crime watch survey," 2005, p. 14). However, given the difficulties involved and the lack of accepted accounting practices, problems with the accuracy of these estimates are widely acknowledged.

If we are resigned to living with rough estimations, can we make the estimating process more transparent and accessible? In this initiative, we call for a more systematic survey of techniques currently in use to estimate financial losses associated with various categories of security incidents and if possible, the development of a consensus on concerning how losses can be estimated.

For example, if a sufficient number of cases of incidents were examined it might be possible to develop a useful formula based on total revenues (or budget), number of employees and extent of IT use to support the organizational mission to calculate an expected loss for incidents resulting from the threat categories identified under the first initiative. We see such heuristics as being somewhat analogous to the advertising industry's use of Nielsen ratings for the purchase of television advertising. The quality of these ratings is widely recognized as suspect, yet advertisers invest billions of dollars each year based, at least in part, on these ratings ("Nielsen Ratings," 2006).

Initiative 3. Develop and Maintain Knowledge Base of Probability Estimates Associated with Threat Classes

The third initiative closely resembles the second in that its primary intent is the collection, consolidation and presentation of expert information. In this case, we are concerned primarily with the estimation of probabilities associated with various threats and threat categories.

While it is possible to find publicly-available threat probability estimates, the effort to do so is non-trivial and the quality of the estimates identified are uncertain and often dated. We were unable to identify a single authoritative source of relevant and current threat data, meaning that interested parties will need to search a variety of sources to obtain the required information. Furthermore, the identification and categorization of threat data may not align well with the threat analysis model in use. Again, we acknowledge that some consulting firms and vendors of security analysis products do maintain such data repositories for those able to pay for access.

The largest problem, though, is the ambiguity regarding source and quality of estimates used regardless of whether the data is public or proprietary. For example, one paper presented at a national-level security conference that reported "exposure/impact coefficients" for a large number of threats, advised "These values were derived using the combined experience and skills of a number of experts in the arena of information systems security" (Meritt, 1999, p. 11). Concerning a commercial implementation of CRAMM, the promotional literature stated, "Now Insight has further enhanced CRAMM by incorporating its knowledge base from hundreds of worldwide consultancy assignments…" ("CRAMM v5.1 information security toolkit," 2006, p. 1).

We certainly do not object to the use of expert knowledge to create these estimates. However, there is no basis provided on which to validate the claims of expertise. How many experts were consulted? How much relevant experience do they possess? Is their expertise relevant to my particular industry or organizational needs? What level of variance in opinions is hidden within these aggregated or negotiated estimates? How often are the knowledge bases updated?

Besides the lack of transparency regarding these data, the cynical among us recognize that security consultants may have vested interests in overstating risk in order to establish a need for their clients to acquire additional security-related services.

As further discussed in the methods section, we propose an "open process" for developing a security vulnerability and threat knowledgebase that:

- Encourages much broader participation in the knowledgebase than what any individual firm or organization would likely be able to achieve
- Provides process transparency so that potential users are able to evaluate the methods used to aggregate and present data
- Includes trend and variance data so that users are able to adjust their use of the data to better align with their organizational needs and culture, e.g., support the conduct of sensitivity analyses based on more or less pessimistic assumptions concerning threats

We believe it would be possible to construct a web-based portal that would identify risk or threat categories (consistent with simplified reference model outlined under initiative 1) allow individuals to enter their estimates of the probabilities associated each category. The site would generate statistics, e.g., number, of participants, mean, median, standard deviation, so that possible consumers of the data could analyze for themselves the source of the data and make their own determinations of how to employ the data. Research has provided evidence that broadly based *prediction markets* may provide a more accurate means of dealing with the multiple layers of uncertainty than the assessments of experts (Hanson, 2003; Surowiecki 2005; Wolfers & Zitzewitz, 2004).

In keeping with the philosophy of simplicity reflected under the first initiative, we do not wish to duplicate the vulnerability databases in existence, e.g., the National Vulnerability Database sponsored by the Department of Homeland Security (DHS) Cyber Security Division/US CERT and maintained by NIST at http://nvd.nist.gov/. We would anticipate the work proposed here would both consume data from and contribute data to open sources of information.

Initiative 4. Develop Automated Tools Instantiating the Analysis Methodology, Heuristics, and Knowledgebase

In keeping with the open source philosophy and culture, the fourth initiative would be to create and maintain a suite of automated tools to support the above initiatives. We believe it is possible to develop a quality product that can be effectively employed by SMEs as have other open source projects such as Apache and MySQL.

We see this effort as being intimately aligned with Initiative 1. We intentionally separated the initiatives recognizing that some will be primarily interested in the development and testing of heuristics and models while others would prefer to support the application development effort. Of course, we recognize that good programmers often hold strong opinions regarding the functional design of their efforts. We would certainly hope for and expect at least some overlapping participation in both initiatives.

Program Governance and Acknowledgement of Limitations

As mentioned specifically with respect to initiatives 1 and 4, the success of what we are proposing would depend on close coordination and cooperation among participants in the various initiatives. For example, it is not clear whether model- or knowledgebase- developers would be better situated to recommend the categorization of threats and vulnerabilities that would achieve the objective of creating a parsimonious and easy-to-use model.

The success of such an initiative (particularly with respect to initiatives 2 and 3) is fundamentally dependent upon obtaining broad-based participation. Furthermore, there is a risk that some participants might maliciously attempt to distort the data collected. In view of the types of data that we propose to be collected, we do not see this as a significant issue but recognize that the possibility certainly exists. The more serious threat is that an insufficient number of individuals would choose to participate at all.

The efforts outlined above require coordination and cooperation among researchers and practitioners. Accordingly, we foresee the requirement for a governing organization capable of establishing and maintaining the “conceptual integrity” of the effort by influencing the prioritization of tasks within each of the respective initiatives (Brooks, 1995). As with the Linux development community, there may be literally thousands of programmers generating code that could be included within the Linux standard. However, a smaller number of dedicated enthusiasts, some perhaps receiving corporate or academic support, continue to serve as architects who evaluate and ultimately decide what features and code will be incorporated (within the Linux kernel). Numerous open source projects have initiated (explore sourceforge.net) and numerous governance mechanisms are employed in support of what are often quite complex development efforts. We have not at this time investigated how such a governance structure might be established and operated. But we believe there are two general models possible. Perhaps the most desirable would be for an existing group or association to provide a degree of institutional support and advocacy for the project, e.g., the SANS Institute or the Association of Information Systems. The advantage of such an approach would be the early identification of resources to kickstart the effort and an ability to leverage the organization's existing governance structure. However, we also believe it possible for a community to self-organize. This potential has been repeatedly demonstrated in the open source community although we admit the number of projects failing to research fruition likely exceeds the number of successful development efforts.

Desirability of Adopting an Open Development Approach

Multiple factors contribute to our recommendation of employing an "open source" approach for implementing this effort. Certainly, an open source approach can be expected to complicate program governance. Furthermore, given the anticipated scope of the program, we confess that our use of the term may be metaphorical as well as literal. For example, model and knowledge base developments may choose to rely on Wiki technology and methods, emphasizing content sharing and management over the development of code.

Foremost among our admittedly untested assumptions is a belief that the quality of each initiative will greatly benefit by broad participation. We would encourage a broad marketplace of ideas where numerous approaches are broached and then incorporated into the approach by general consensus. The process should be open and accessible such that even after an approach is adopted, there is ample opportunity for criticism and dissent; a moderated "Darwikinism" process (Lamb, 2004, p. 42).

While we accept the necessity of a governance function to maintain conceptual integrity and help the community move toward actual delivery of functional capabilities, we also anticipate that a broadly based effort will spawn offshoots that, while potentially valuable, simply do not fit within the scope of the effort as initially conceived and accepted by the community of participants.

Secondly, we are committed to the idea of the free distribution of whatever knowledge results from these efforts. This desire should not be interpreted as an anti-business stance. We are simply aware that many organizations have not yet been motivated or able to expend the financial resources required to obtain quality assistance in determining their security needs. The failure of these many organizations to adopt improved IA practices can have adverse economic consequences. Additionally, we believe that the availability of the knowledge created may help drive the improvement of commercial products as vendors seek to maintain commercially viable products.

Implications of Proposal in Terms of an Interdisciplinary Research Agenda

While the program outlined above could be well orchestrated by a community consisting primarily of security practitioners, its implementation presents a myriad of research opportunities ranging from the strictly applied to the highly theoretical. Just a few are outlined below.

- A fundamental motivation for proposing this effort is a belief that there are cognitive and cultural as well as financial factors influencing the extent and quality of security practice adoption (Cline & Jensen, 2004; Jahner & Krcmar, 2005; Rhee, Young, & Kim, 2005). We are particularly interested in the further exploration of individual (cognitive) and group behaviors that impede effective adoption and use of recognized security management "best practices." In addition to the *optimistic bias* and *illusion of control* investigated by Rhee et al. (2005), a wide range of investigations have been conducted to analyze determinants of *decision avoidance* behavior (Anderson, 2003). In particular, application of research studying *effort-accuracy* (Luce, Bettman & Payne, 1997; Payne, 1982), tradeoffs and *information overload* (O'Reilly, 1980) could prove useful for identifying optimal levels of abstraction for use in designing the proposed models. That is, at what level of model complexity does its usage significantly decline? It is not enough to develop models and applications; their adoption and use (and non-adoption and non-use) will need to be studied.

- The development and evaluation of theory-based threat models should apply rigorous theoretical and empirical methods to validate or correct the intuitive assessments of security consultants, "to raise the discussion above the level of folklore and into the realm of science (Straub & Welke, 1998). For example, Ramachandram and White (2004) have presented a Complementarity Based First Order Effects (CoBFOE) to determine benefits of security-related investments, and Locher (2005) examines the implication of Basel II regulations for financial institutions on the conduct of IS-related risk analyses.
- Given concerns regarding quality of data available to practitioners for conducting risk analyses and the difficulties inherent in developing accurate and reliable estimates, specific investigation is warranted into the processes by which these data are developed and what techniques might be useful to improve quality. While some current threat probability estimates are derived from actuarial data (e.g., natural disasters, fire) and some are derived from surveys (e.g., Gordon, Loeb, Lucyshyn & Richardson, 2005), the evidence cited above suggests that many of the estimates used are products of expert analysis and intuition. While Delphi approaches have long been used for investigating complex problems (Turoff & Linstone, 2002), research in the area of *prediction markets* may provide a more accurate means of dealing with the multiple layers of uncertainty inherent in the risk analysis process (Hanson, 2003; Wolfers & Zitzewitz, 2004).

The above topics reflect some of the interests and initial thinking of the authors regarding research opportunities that could be derived from and benefit the proposed initiatives. Certainly, many other research opportunities could be identified.

Conclusion and Call to Action

Spending on IS security is expected to exceed $30 billion this year. Yet, in spite of these investments, losses in excess of $15 billion are anticipated to occur because of security breaches (Mooney, Chun, Hovav, George, & Griffy-Brown, 2005). Current IS security research and practice is dominated by development of ever more sophisticated technologies for security control and compromise detection. However, "there is a relative dearth of insights that help firms to understand the socio-organizational challenges of managing the deployment and use of these tools to prevent IS security compromises" (Mooney et al., 2005, p. 3627).

In keeping with the spirit of the 2005 AMCIS panel evaluating security theory and practice and Whitman and Mattord's (2003, p. 33) discussion of information security as "an art or a science," the initiatives outlined above specify a pragmatic course of action intended to combine the efforts of scholars and practitioners in a rigorous and relevant assault on the complex social and technical issues specifically associated with IA/security risk management and analysis.

The underlying logic of our suggested approach is based on creating an open and transparent process to develop relatively simple abstract models and heuristics to aid in security related decision making. Additionally, we want to make expert estimates concerning threat probabilities and cost calculations associated with asset exposure publicly available to assist organizations in effectively applying the model(s). We recognize that this approach may present legitimate concerns regarding the quality of the analyses. However, quality assessments can be made by subjecting the models to empirical verification.

We recognize that when viewed in total, the success of our proposal is highly dependent upon numerous and willing participants. We believe that the open source community and the success of Wikipedia provide ample evidence that such participation is possible, although certainly not assured. We have attempted to outline a multifaceted approach that will appeal to pragmatically oriented security practitioners as well as academicians interested in pursuing theoretically rigorous research within the area of information security. The authors are interested in hearing from those who willing to further explore proposals outlined in this article.

References

2005 E-crime watch survey: Summary of findings. (2005). Retrieved 9 February 2006 from http://www.cert.org/archive/pdf/ecrimesummary05.pdf

Alberts, C., & Dorofee, A. (2002). *Managing information security risks: The OCTAVE(sm) approach*. Boston, MA: Addison-Wesley.

Anderson, C. J. (2003). The psychology of doing nothing: Forms of decision avoidance result from reason and emotion. *Psychological Bulletin*, *129*(1), 139-167.

Brooks, F. P. (1995). *The mythical man-month: Essays on software engineering*. Reading, MA: Addison-Wesley.

Cline, M., & Jensen, B. K. (2004). *Proceedings of the Tenth Americas Conference on Information Systems* (pp. 4514-4520). New York, NY: Association for Information Systems.

CRAMM v5.1 information security toolkit. (2006). Retrieved 10 February 2006 from http://www.insight.co.uk/files/datasheets/CRAMM%20(Datasheet).pdf

Dutta, A., & Roy, R. (2003). The dynamics of organizational information security. In *Proceedings of the Twenty-fourth International Conference on Information Systems* (pp. 921-927). Seattle, WA: Association for Information Systems.

Gordon, L. A., Martin, L., P., Lucyshyn, W., & Richardson, R. (2005). *CSI/FBI computer crime and security survey*. Retrieved 31 January 2006 from http://www.gocsi.com/forms/fbi/csi_fbi_survey.jhtml

Hanson, R. (2003). Combinatorial information market design. *Information Systems Frontier*, *5*(1), 107-119.

Harper, E. (2002). OCTAVE developers reach out to smaller organizations with OCTAVE-S. *News@sei* (Online), *5*(5). Retrieved 9 February 2006 from http://www.sei.cmu.edu/news-at-sei/features/2002/4q02/feature-1-4q02.htm

Jahner, S., & Krcmar, H. (2005). Beyond technical aspects of information security: Risk culture as a success factor for IT risk management. In *Proceedings of the Eleventh Americas Conference on Information Systems* (pp. 3327-3336). Omaha, NE: Association for Information Systems.

Jaquith, A. (2007). *Security metrics: Replacing fear, uncertainty, and doubt*. Upper Saddle River, NJ: Addison-Wesley Pearson Education

Lamb, B. (2004). Wide open spaces: Wikis, ready or not. *EDUCAUSE Review*, *39*(5), 36-48.

Locher, C. (2005). Information systems in a rapidly changing economy. In *Proceedings of the 13th European Conference on Information Systems*. Regensburg, Germany: ECIS.

Luce, M. F., Bettman, J. R., & Payne, J. W. (1997). Choice processing in emotionally difficult decisions. *Journal of Experimental Psychology*, *23*(2), 384-405.

McCumber, J. (2005). *Assessing and managing security risk in IT systems: A structured methodology*. Boca Raton, FL: Auerbach Publications.

Meritt, J. W. (1999). A method for quantitative risk analysis. In *Proceedings from the 22nd National Information Systems Security Conference* (Online). Retrieved 9 February 2006 from http://csrc.nist.gov/nissc/1999/proceeding/papers/p28.pdf

Mooney, J., Chun, M., Hovav, A., George, J., & Griffy-Brown, C. (2005). Are prevailing theories and practices of IS security management adequate? An evaluation and call to action. In *Proceedings of the Eleventh Americas Conference on Information Systems* (p. 3627). Omaha, NE: Association for Information Systems.

National Institute of Standards and Technology. (2002). Special Publication *Risk management guide for information technology systems* (800-30). Washington, DC: U.S. Government Printing Office.

Nielsen Ratings. (2006). Retrieved 9 February 2006 from http://en.wikipedia.org/wiki/Nielsen_Ratings

O'Reilly, C. A. (1980). Individuals and information overload in organizations: Is more necessarily better? *Academy of Management Journal*, *23*(4), 684-696.

OCTAVE methods. (2003). Retrieved 9 February 2006 from http://www.cert.org/octave/methods.html

Payne, J. W. (1982). Contingent decision behavior. *Psychological Bulletin*, *92*, 382-402.

Peltier, T. R.. (2005). *Information security risk analysis* (2nd ed.). Boca Raton, FL: Auerbach Publications.

Ramachandran, S., & White, G. B. (2004). Methodology to determine security ROI. In *Proceedings of the Tenth Americas Conference on Information Systems* (pp. 4423-4432). New York, NY: Association for Information Systems.

Rhee, H.-S., Young, R. U., & Kim, C.-T. (2005). I am fine but you are not: Optimistic bias and illusion of control on information assurance. In *Proceedings of the Twenty-sixth International Conference on Information Systems,* pp. 381-394. Las Vegas, NV: Association for Information Systems.

RiskWatch: Information systems & ISO 17799 2005 Product Sheet. (2005). Retrieved 31 January 2006 from http://www.riskwatch.com/ProductSheets/RW-IS_Product_Flyer_0705.pdf

Schneier, B. (2004). *Secrets & lies: Digital security in a networked world*. Indianapolis, IN: Wiley Publishing.

Simon, H. A. (1996). *The science of the artificial* (3rd ed.). Cambridge, MA: MIT Press.

Sourceforge.net FAQ. (2006). Retrieved from http://sourceforge.net/docs/about

Storey, D. J. (2003). Entrepreneurship, small and medium sized enterprises and public policies. In Z. Acs & D. B. Audrestch (Eds.), *Handbook of entrepreneurship research: An interdisciplinary survey and introduction* (pp. 473-511). Great Britain: Kluwer Academic Publishers.

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

Surowiecki, J. (2005). *The wisdom of crowds*. U.S.A.: Anchor Books

Turoff, M., & Linstone, H. A. (2002). *The Delphi method: Techniques and applications*. Retrieved 25 January 2006, from New Jersey Institute of Technology: http://www.is.njit.edu/pubs/delphibook/.

Whitman, M. E. (2003). Enemy at the gate: Threats to information security. *Communications of the ACM, 46*(8).

Whitman, M. E., & Mattord, H. J. (2003). *Principles of information security.* Boston, MA: Thomson Course Technology.

Wolfers, J., & Zitzewitz, E. (2004). Prediction markets. *Journal of Economic Perspectives*, *18*(2), 107-126.

Biographies

John C. Beachboard joined the Computer Information Systems faculty at Idaho State University in 2001. He completed the Ph.D. in Information Transfer and the M.S. in Information Resources Management at the School of Information Studies, Syracuse University. He holds an M.S. in Business Administration from Boston University and a B.S. in Public Administration from the University of Arizona. Dr. Beachboard has taught graduate courses in research methods, project management, and IT use in business, and undergraduate courses in IT management and systems architectures. He has held staff and management positions developing, implementing and operating information and telecommunications systems for the Department of Defense. He is keenly interested in the development, application and effectiveness of information technology management policies in the private and public sectors.

At the time of writing, **Alma R. Cole** was graduate student working toward his M.S. in Business Administration with an emphasis in Information Assurance which he received in 2007. He completed a B.S. in Business Information Systems with an E-Commerce Emphasis from Utah State University. His experience includes work as an IT Analyst with the Government Accountability Office (GAO) and as an IT Security Analyst with National Information Assurance Training and Education Center (NIATEC). Alma is an International Information Systems Security Certification Consortium (ISC)² Certified Information Systems Security Professional (CISSP) and System Security Certified Practitioner (SSCP). His topics of interest include risk management, incident response, business continuity, information security policy, and enterprise network security. Alma is currently employed as an IT Security Specialist by the Department of Homeland Security.

Michael L. Mellor is currently employed as an Information Security Architect at the Centers for Medicare and Medicaid Services within the Federal Government. Michael completed an M.S. in Business Administration at Idaho State University where he also specialized in Information Security. He also holds a B.S. in Business Information Systems from Utah State University. Michael has numerous Information Security certifications including a CISSP, SSCP, NSA IEM, NSA IAM, and a Security+.

Steven G. Hernandez, CISSP, SSCP, is an information assurance professional presently working in the Washington DC area. He completed his MBA in Computer Information Systems and Information Assurance at Idaho State University. He also holds a BBA in Computer Information systems from Idaho State University and degrees in electronic systems, lasers, and electro-optics. Through his work with the National Information Assurance Training and Education Center, Hernandez has lectured on topics in information assurance, risk management, capital planning and investing in security, certification and accreditation, and the business justification of certification and accreditation to graduate level audiences. Hernandez chairs a position on Scholarship for Service Cyber Corps Alumni board of directors, and is actively involved in educational content development for the International Information Systems Security Certification Consortium. His present interests include identity management in the federal government, IT security in federal contract law, risk management through collaborative diversification of IT infrastructure, and how organizations can transfer risk.

Kregg Aytes has been a member of the Computer Information Systems faculty at Idaho State University since 1993. He completed his Ph.D. at the University of Arizona in that same year. Kregg teaches graduate and undergraduate courses in CIS, and has been department chair since 2000. He research interests include information security and collaborative technologies. He also has a strong love of teaching and is interested in the application of IS content and skills across the business school curriculum.

Nelson Massad joined the Department of Information Technology and Operations Management at Florida Atlantic University in August, 2003. He received a B.S. in Computer Science from Beirut University College in 1989, a M.S. in Computer Science from the University of San Francisco in 1992, a M.S. in Telecommunications and Network Management from Syracuse University in 2003, and a Ph.D. in Information Science and Technology from Syracuse University in 2003. Dr. Massad's research interest is mainly in the electronic commerce area, exploring the role of individual transactions in customer relationship management. More recently, Dr. Massad has been involved in the area of information assurance, exploring the ways that small to medium size companies conduct risk analyses. Dr. Massad has taught a variety of courses, including an introduction to management information systems course, introductory and intermediate programming courses using C++, advanced programming courses using C# and the .NET framework, and a course on quantitative methods in business administration.