Statement on Research
Eliot Rich
Fall 2009

My research looks for patterns and structures of organizational behavior in the domains of technology management, computer security and infrastructure vulnerability. Case study alone results in rich detail and low generalizability [1]. In my targeted domains, grounded research often produces confidential results that cannot be disseminated beyond those involved with the problem in question. I combine case study with System Dynamics simulation to develop causal abstractions and testable hypotheses [2]. The combination of case study and simulation modeling helps develop and explore theory for practice while preserving the confidentiality of informants and supporting inductive theory-building.

I used this approach first in my dissertation to examine knowledge management program sustainability. Subsequently, I began applying this technique to the domains of information security and critical infrastructure, two areas where an integrated socio-technical perspective is needed [3-5]. My collaborators and I apply knowledge elicitation and group model building techniques [6] that provide causal insight without unmasking sensitive operational details. We have employed this approach to insider cyber-threats [7, 8], energy infrastructure safety [9-13], and are currently working on a multi-year study of attack scenarios against the pan-European electric power grid.

While my research spans a number of applications, the underlying constant is the use of simulation and systems thinking to better understand and influence strategic policy effectiveness. I anticipate that these efforts will generate interesting and fruitful research for some time.

Knowledge Management

My dissertation work on knowledge management in consulting firms has been the source of two publications, co-authored with my advisor, Prof. Peter Duchessi. The first paper examines knowledge management programs at two international consulting companies. Using interviews, secondary document analysis, and simulation, I demonstrate that initially successful knowledge management programs degrade and have difficulty sustaining value under a wide set of conditions [14]. The paper was nominated for the HICSS Conference's Best Paper Award. The second product from my dissertation is a synthetic case study, which presents a decision-maker's view on knowledge management program sustainability [15], and was reprinted in an omnibus collection on knowledge management [16]. The dissertation has been cited for its use of qualitative interview techniques to review the findings of quantitative simulation models when first-hand structure and data are both lacking, thereby opening a new approach to model validation and theory building [17].

The use of dynamic models to understand the effects of knowledge on organizational security is a natural extension of this early work. I have co-authored two journal publications [18, 19] with Dr. Finn Olav Sveen, University at Agder, Norway, that discuss how unseen staffing and information dynamics can improve or degrade organizational security over time.

System Dynamics Modeling of Infrastructure and Cyber Threats

In 2004 I began a stream of research that examined emergent threats to infrastructure and computer security through the lens of system dynamics. While most research in the field looks at technical measures for detection and prevention, there is a growing interest in the softer side of security and compliance. In this regard, key security researchers have noted that compliance is often seen as in conflict with operational productivity. My collaborators and I used confidential empirical data to identify a "win-win" business case and theoretical support for greater security compliance.

These works were created in collaboration with Carnegie Mellon University's Computer Emergency Response Team / Coordination Center (CERT/CC), the national clearinghouse for computer attacks, mitigation, and intervention. In our joint papers we develop a causal theory surrounding the development and exploitation of insider opportunities and threats [7, 8]. Our theoretical work is an integral part of CERT/CC's research and protection strategy, as evidenced by their development of a body of work referencing our initial collaboration [20, 21].

Dr. Ignacio Martinez-Moyano of Argonne National Laboratory, Dr. Stephen Conrad of Sandia National Laboratories and I later combined judgment theory and signal detection theory to posit a dynamic model of how decision-makers may be affected by partial and incomplete information. This type of decision process is present in many security activities, where decisions about screening or signal interpretation are enmeshed in uncertainty and delay [22].

A related line of research is the examination of vulnerability black markets. There is a smoldering concern among security researchers about marketplaces where software exploits may be bought and sold. These exploits could then be launched against corporate or government targets. Professor Jose J. Gonzalez and Ms. Jaziar Radianti of Agder University, Norway, and I first presented a dynamic theory of such markets [23], followed by empirical analyses [24, 25]. I am co-supervising Ms. Radianti's dissertation.

The modeling work in cyber-threats at CERT/CC led to an invitation to work with Prof. Gonzalez on a project that linked cyber-security and infrastructure protection in mission-critical operations. The Norwegian Oil Ministry and OLF, the Norwegian oil industry consortium, are concerned about how the introduction of computer and network-facilitated tools for improved profitability would affect the safety of its off-shore oil platforms. These platforms, which collectively represent the world's fourth-largest source of energy products, face continuous vulnerability from engineering and human failures.

I was part of a three-person team that planned and executed two week-long group model building exercises that linked energy platform vulnerability and transition speed. We constructed models that illustrate the range of economic effects that might occur if the transition was implemented faster than their ability to manage unidentified but expected problems that only fieldwork could uncover. The particularly innovative part of this effort was modeling the cumulative effects of process change where there was scant historical information. This work has been presented in academic conferences and industry publications [9-12], with the first journal paper appearing in 2009 [13] and a second paper under review. In 2007 I addressed the Integrated Operations

industry conference in Trondheim, Norway as part of my on-going research collaborations with SINTEF, the largest independent research organization in Scandinavia, where we apply dynamic modeling to operational safety analysis [26].

The combined case study and simulation approach to complex systems is currently being applied in the SEMPOC research program, based at TECNUN, University of Navarra, Spain. We use these techniques to consider how the effects of a multi-national power crisis might cascade across the European Union. My specific role is the design and implementation of the group modeling processes and simulation reviews, working with experts and scientists from across the European Union. Our first publication, describing our research approach, is currently under review.

Information Technology and Innovation Management

My work in socio-technical systems includes consideration of the social and organizational structures needed to support and sustain innovations. I recently published an article on the role of information delays in management fads [27]. Through simulation I demonstrate how uncertain outcomes and deployment delays can create the boom and bust behavior often seen in management fads.

Information delays also play a role in the implementation of large IT projects, where organizations may over-commit to a project beyond its reasonable capability for completion. A paper on the repeating cycles of project over-commitment at the US Internal Revenue Service with Dr. Mark Nelson and Mr. Andrew Whitmore of UAlbany is under first review.

A different type of information delay was found in my case study of E-ZPass implementation issues [28]. Here I used secondary data and expert interviews to describe the issues surrounding the implementation of E-ZPass on the Ohio Turnpike. The analysis shows that the supervising organization was slow to realize the effects of changes in toll structures on the surrounding communities. These changes created political pressures that further disrupted the economic stability of the roadway. This case was originally written for teaching systems analysis and design within UAlbany.

A comparative case study of electronic voting security architectures, authored by Dr. Guido Schryen and myself, shows weaknesses in the implementation of innovative voting technology [29], Dr. Schryen will be coming to Albany in 2010 for an 18 month post-doctorate position under the direction of Prof. David Andersen and myself.

Another methodological contribution of my portfolio is a nascent investigation of the semantic characteristics of the IT research literature. This research is aimed at narrowing the variability found in survey- and interview-based data by looking at semantically similar and dissimilar structures. I presented a paper co-authored by Professor Kai Larsen of University of Colorado and Professor Dorit Nevo of York University, Canada, outlining the analytical approach [30]. We have a proposal to the NSF under review, following an initial attempt for similar funding in 2008.

In addition, I am a participant in the School of Business "Going Green Globally" project. This cornerstone program combines simulation exercises, classroom activities and fieldwork with business clients. I provide students with tools for systems thinking and holistic models of sustainable green businesses. We presented our results at a developmental conference in Fall 2009, with a journal submission planned for later in the year.

Prospects for the future

For the last six years I have been studying knowledge management, information security, and critical infrastructure. These topical areas share a sense of urgency and focus that opens opportunities for research. I perform this work by structuring both the problem and problem-solving dialogue through causal and simulation modeling. The generalizable academic contribution continues through the reflection and experimentation with models and concepts derived from this grounded approach.

My collaborators and I have been fortunate to receive multiple research grants supporting the development of models for managing crises and mitigating their effects. We have established a productive collaborative research network within the United States and abroad. I anticipate that we will be able to continue publishing useful and insightful research for years to come.

References

[1] K. M. Eisenhardt and M. E. Graebner, "Theory building from cases: Opportunities and challenges," *Academy of Management Journal*, vol. 50, pp. 25-32, 2007.

[2] J. D. Sterman, *Business dynamics: Systems thinking and modeling for a complex world*. Boston: Irwin/McGraw-Hill, 2000.

[3] G. Dhillon and J. Backhouse, "Current directions in IS security research: towards socio-organizational perspectives," *Information Systems Journal*, vol. 11, p. 127, 2001.

[4] Infosec Research Council, "Hard Problem List," November 2005. Available at http://www.infosec-research.org/docs_public/20051130-IRC-HPL-FINAL.pdf.

[5] Computer Science and Telecommunications Board, *Towards a safer and more secure cyberspace*. Washington, DC: National Academies Press, 2007.

[6] J. A. M. Vennix, *Group model building: Facilitating team learning using system dynamics*. Chicester: John Wiley & Sons, 1996.

[7] D. F. Andersen, D. Cappelli, J. J. Gonzalez, M. Mojtahedzadeh, A. Moore, E. Rich, J. M. Sarrigui, T. J. Shimeall, J. Stanton, E. A. Weaver, and A. Zagonel, "Preliminary system dynamics maps of the insider cyber-threat problem," in *the 22nd International Conference of the System Dynamics Society*, Oxford, UK, 2004.

[8] E. Rich, I. J. Martínez-Moyano, S. H. Conrad, D. M. Cappelli, A. P. Moore, T. J.

Shimeall, D. F. Andersen, J. J. Gonzalez, R. J. Ellison, H. Lipson, D. Mundie, J. M. Sarriegi, A. Sawicka, T. R. Stewart, J. M. Torres, E. A. Weaver, and J. Wiik, "Simulating Insider Cyber-Threat Risks: A Model-Based Case and a Case-Based Model," in *Proceedings of the 23rd International Conference of the System Dynamics Society*, Boston, 2005, pp. 126-127.

[9] E. Rich, "Modeling Risk Dynamics in e-Operations Transitions," in *3rd International ISCRAM Conference*, Newark, NJ, 2006.

[10] E. Rich and J. J. Gonzalez, "Maintaining Security and Safety in High-threat E-operations Transitions," in *39th Hawaii International Conference on System Sciences*, Kauai, Hawaii, 2006.

[11] E. Rich, F. O. Sveen, Y. Qian, S. A. Hillen, J. Radianti, and J. J. Gonzalez, "Emergent Vulnerability in Integrated Operations: A Proactive Simulation Study of Risk and Organizational Learning," in *40th Hawaii International Conference on System Sciences (HICSS-40)*, Big Island, Hawaii, 2007.

[12] J. J. Gonzalez, Y. Qian, F. O. Sveen, and E. Rich, "Helping Prevent Information Security Risks in the Transition to Integrated Operations," *Telektronikk*, vol. 101, pp. 29-37, 2005.

[13] E. Rich, J. J. Gonzalez, Y. Qian, F. O. Sveen, J. Radianti, and S. Hillen, "Emergent vulnerability in Integrated Operations: A proactive simulation study of economic risk," *International Journal of Critical Infrastructure Protection*, vol. 2, pp. 110-123, 2009.

[14] E. Rich and P. Duchessi, "Modeling the sustainability of knowledge management programs," in *Proceedings of the Hawai'i International Conference on System Sciences (HICSS-37)*, Big Island, Hawaii, 2004.

[15] E. Rich and P. Duchessi, "Keeping the Flame Alive: Sustaining a Successful Knowledge Management Program," in *Case Studies in Knowledge Management*, M. Jennex, Ed. Hershey, PA, USA: Idea Group, 2005.

[16] E. Rich and P. Duchessi, "Keeping the Flame Alive: Sustaining a Successful Knowledge Management Program," in *Knowledge Management: Concepts, Methodologies, Tools and Applications*, M. Jennex, Ed. Hershey, PA, USA: IGI Global, 2007.

[17] L. F. Luna-Reyes and D. L. Andersen, "Collecting and analyzing qualitative data for system dynamics: Methods and models," *System Dynamics Review*, vol. 19, pp. 271-296, 2003.

[18] F. O. Sveen, E. Rich, and M. Jager, "Overcoming Organizational Challenges to Secure Knowledge Management," *Information Science Frontiers*, vol. 9, pp. 481-492, 2007.

[19] F. O. Sveen, J. M. Sarriegi, E. Rich, and J. J. Gonzalez, "Toward viable information security reporting systems," *Information Management & Computer Security* vol. 15, pp.

408-419, 2007.

[20] D. Cappelli, A. Moore, and T. Shimeall, "Common Sense Guide to Prevention and Detection of Insider Threats," Cylab, Carnegie Mellon University, Pittsburgh, PA April 2005.

[21] D. M. Cappelli, A. G. Desai, A. P. Moore, T. J. Shimeall, E. A. Weaver, and B. J. Willke, "Management and education of the risk of insider threat (MERIT): System dynamics modeling of computer system sabotage," in *The 25th International System Dynamics Conference*, Boston, MA, 2007.

[22] I. J. Martinez-Moyano, E. Rich, S. Conrad, T. Stewart, and D. F. Andersen, "Integrating judgment and outcome decomposition: Exploring outcome-based learning dynamics," in *24th International Conference of the System Dynamics Society*, Nijmegen, The Netherlands, 2006.

[23] J. Radianti, E. Rich, and J. J. Gonzalez, "Using a Mixed Data Collection Strategy to Uncover Vulnerability Black Markets," in *Workshop for Information Security and Privacy*, Montréal, Canada, 2007.

[24] J. Radianti, J. J. Gonzalez, and E. Rich, "A quest for a framework to improve software security: Vulnerability Black Market scenario," in *27th International Conference of the System Dynamics Society*, Albuquerque, NM, USA, 2009.

[25] J. Radianti, E. Rich, and J. J. Gonzalez, "Vulnerability Black Markets Empirical Evidence and Scenario Simulation," in *42nd Hawaii International Conference on System Sciences*, Big Island, Hawaii, 2009.

[26] S. O. Johnsen, C. W. H. Hansen, M. B. Line, Y. Nordby, E. Rich, and Y. Qian, "CHECKIT-A Program to Measure and Improve Information Security and Safety Culture," *International Journal of Performability Engineering,* vol. 3, pp. 175-186, 2007.

[27] E. Rich, "Management Fads and Information Delays: An Exploratory Simulation Study," *Journal of Business Research,* vol. 61, pp. 1143-1151, 2008.

[28] E. Rich, "E-ZPass and the Ohio Turnpike: Adoption and Integration of Electronic Toll Collection," *Journal of Cases on Information Technology,* vol. 10, pp. 32-51, 2008.

[29] G. Schryen and E. Rich, "Security in Large-Scale Internet Elections: A Retrospective Analysis of Elections in Estonia, The Netherlands, and Switzerland," *IEEE Trans. on Information Forensics and Security,* in press.

[30] K. Larsen, D. Nevo, and E. Rich, "Exploring the Semantic Validity of Questionnaire Scales," in *Hawaii International Conference on System Sciences (HICSS-41)*, Big Island, Hawaii, 2008.