Association for Information Systems
AIS Electronic Library (AISeL)

WISP 2012 Proceedings

Pre-ICIS Workshop on Information Security and Privacy (SIGSEC)

Winter 12-15-2012

Information Security Policy Development Through the Lens of the Institutional Analysis and Development Framework

Susan M. Jones
Utah State University, susan.jones@usu.edu

Katherine M. Chudoba
Utah State University

Information Security Policy Development Through the Lens of the Institutional Analysis and Development Framework

Susan M. Jones[1]
Jon M. Huntsman School of Business, Utah State University,
Logan, UT, USA

Katherine M. Chudoba
Jon M. Huntsman School of Business, Utah State University,
Logan, UT, USA

ABSTRACT

Organizations worldwide are increasing their information security initiatives to keep pace with the highly complex and dynamically changing operating environments. With mounting regulations, risk mitigation, and critical information protection pressures, they focus on IT governance. Using a case study methodology, this research in progress introduces an interdisciplinary common governance framework to information security policy, an important internal governance control. The Institutional Analysis and Development (IAD) framework is part of Nobel Prize-winning work in economics and is recognized as one of the most comprehensive tools for both design and analysis of policy interventions.

Keywords: policy development, IAD framework, information security, institutions

INTRODUCTION

Securing operations is a key managerial function that must be emphasized if organizations are to maintain their resiliency (ITGI 2011; OMB 2010; Peterson 2004). Failure to adequately govern and secure computerized resources leaves organizations vulnerable to damaging information breaches (Campbell et al. 2003). The pervasiveness of IT, the dependency on IT, the inherent risks of IT, and the investment in IT, all point to the critical focus

[1] Corresponding author. susan.jones@usu.edu. +1 435 797 2288

on IT governance (van Grembergen and De Haes 2008), and the importance of an information security policy with adequate internal controls is critical (Box 2010).

An increased number of academic studies have focused on end user or managerial intentions (Bulgurcu et al. 2010; D'Archy et al. 2009; Siponen and Vance 2010; Warkentin et al. 2011), and policy-making prescriptions have been introduced in the form of information security policy guidelines and checklists (COBIT 2011; ISO/IEC 2005; NIST 1996, 1995). This renewed focus is a positive attempt to find new ways of improving the overall security in the organization by involving the end user (Dinev and Hu 2007). Research in information systems and in information security has neglected the interlocking systems of managers and end users, and their varying intentions (Siponen and Willison 2009). Hence, a comprehensive, theoretical governance approach is needed to understand how policy participants structure their interactions with respect to their environments and to the information and knowledge resources they utilize and produce.

Common governance has long struggled with the relationship between institutions and policy making, as well as the relationship between policy making and policy outcomes (Sabatier 2007). Ostrom (2005, 1990) contends that researchers should not study the effect of change pertaining to one institution; instead, they must study the relationship produced by institutional change, meaning in effect they must look at the context of all institutions. The Institutional Analysis and Development (IAD) framework is one such tool that offers significant potential for learning within and across the policy phenomena (Madison et al. 2008). The framework is an outcome of the collaboration of Ostrom and scholars who desired a systemic approach for analyzing the social role and significance of cultural institutions that govern sustainable actions and outcomes. The widely empirically tested, interdisciplinary, institutional theory-grounding

framework is praised for its multi-tiered means of organizing policy inquiry into a set of variables (Weible et al. 2012, 2011; Nowlin 2011; Real-Dato 2009; Sabatier 2007; Schlager 2007). Notably, the framework opens connections, comparisons, and analysis that may be otherwise overlooked or separated, thus providing information security policy process with a robust stewardship model.

RESEARCH GOALS, OBJECTIVES, AND QUESTIONS

Since few studies have developed and empirically tested theoretical models of the information security policy process (Whitman 2008), the fundamental overarching argument of this research is that the nature and scope of the information policy process impacts the nature and scope of the information policy and possibly the policy outcome. The IAD framework (see Figure 1) reveals the structure of nested building blocks used to understand human interactions in various settings and situations. The four major areas of the framework include (1) the core analytical action situation that is affected by (2) exogenous variables with the result generating (3) interactions and outcomes as well as (4) feedback (Ostrom 2005).

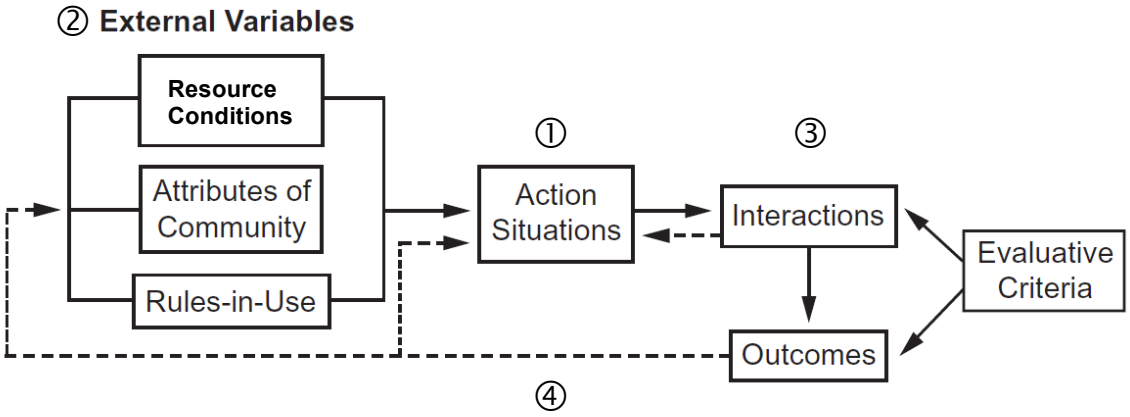

Figure 1. IAD Framework, a Framework for Institutional Analysis
Adapted from E. Ostrom (2011, p. 10)

The "action situation" is the IAD focal point, where actively interested policy actors interact to influence decisions and/or policy design (Real-Dato 2009). Action situations rarely

exist independently of other situations (Ostrom 2005); each is nested within one of three levels or tiers of action—operational, policy (often referred to as collective choice), or constitutional (Ostrom 2011). Recognizing the complexity of the policy process, the three levels play an important role in the integrative approach to effective policy process, resolving the issue argued by Sabatier (1991) that many strands of policy research in the past have been too narrowly focused, including only a single type of institution or organizational level.

The portability of the framework will be particularly helpful for information security scholarship, as the policy level delineations in the IAD framework are consistent with the delineations reflected in common IT security practices in government (NIST 1996, 1995), practice (Whitman and Mattord 2010; Wood 2009), and academic studies (Baskerville and Siponen 2002; Dhillon 2007; White 2009) (see Table 1). In information security policy, each policy type or level has a specific focus, audience, and purpose.

Table 1. Relating Security Policy Terminology with IAD Terminology
Adapted from Dhillon (2007 p. 114-119), NIST SP 800-14, Ostrom (2005), and Whitman and Mattord (2010 p. 122-136)

Policy Relation	Security Policy Type	InfoSec Decision Class	IAD Tier	Policy Topics	Decision Example
Overall Organizational Environment	EISP	Strategic	Policy Tier	Strategic direction, scope, and tone for organization security efforts—corporate philosophy on security	Integrate enterprise system; compliance with corporate governance principles mandated by SOX 2001
Adequate Structures and Processes	ISSP	Administrative	Both Policy and Operational Tiers	Use of process, technology, or systems—a standard of compliance; incident response	Establish responsibilities and authority relating to structures and processes, complying with SOX regulatory bodies, organizational rules, and policies
Optimize Work Patterns	SysSP	Operational	Operational Tier	Managerial guidance and technical specifications	Ensure process integrity, controls, procedures, checks, and balances

This research will take an in-depth look at the first two sections of the IAD framework—the exogenous variables and the action situation—predominantly noting the role of institutions in the process. This initial understanding of elements, including institutions, in information

security policy development will accrue learning and knowledge, opening additional avenues for improving the performance of policies.

The IAD framework will help provide the answers to the following research questions:

1. **What is the nature and scope of the information security policy development process used by security professionals in a large healthcare organization?**
2. At what level—operational, policy, or constitutional—can key elements, observed at the study site, be most productively measured in terms of information security policy development?
3. From evidence obtained at the study site, what specific advances have been made in identifying and analyzing the elements of the information security process with respect to laws and regulations in the healthcare industry?
4. What are the basic relationships among the key elements in the information security policy process, as observed at the study site?
5. What elements or relationships in the policy process, observed at the study site, are most critical in information security policy development?
6. **To what extent does the organization's existing information security policy development process compare to that of the IAD development framework?**
7. What rules are understood and controlled to achieve the anticipated and desired effects within the information security policy process? (March and Olsen 2009 p. 171-172)
8. From the results of semi-structured interviews and document reviews, how do external variables affect the nature and scope of the information security policy development process?

9. What factors observed through the case study facilitated or inhibited policy development in the organization?
10. (a) How do participants in the information security policy process structure their interactions in relation to the policy development environment? (b) What are their preferences, the attributes of the community in which they work, the rules shaping the incentives and constraints they face, and their interactions with other participants?
11. What are the information and incentive structures in the information security policy process, and how do they affect the information security development process?

METHODS

The proposed study involves an exploratory single-case study that will qualitatively search for complex variables in order to understand the process by which policy is formed (Glesne 2006). The qualitative approach allows an in-depth examination of the policy-related phenomenon, while recognizing the issues in their multifaceted forms, dimensions, and layers, without simplifying the phenomenon observed from multiple participants and their individual experiences within an organizational setting (Creswell 2003; Leedy and Ormrod 1985). The approach is appropriate as information security policy process has limited research and needs detailed exploration and understanding of how participants structure their interactions, advancing both practice and literature (Gall et al. 2007). Also, the approach is consistent with the prior studies conducted with the IAD framework.

According to Benbasat et al. (1987), much insight can be gained from case study research, especially when the research is not preceded by numerous related studies. This case study comprises an all-encompassing method, which covers the logic of design, data collection techniques, and specific approaches to data analysis (Yin 2003).

Data will be collected using multi-methods (i.e., interviews, observations, document reviews) to strengthen the results through triangulation (Creswell 2003; Kaplan and Duchon 1988; Yin 2003). Since qualitative research is assessed on the quality and rigor of the research (Creswell 2003; Yin 2003; Guba and Lincoln 2005), Tables 2 and 3 briefly identify the validity and the reliability criteria important to the credibility of this case study.

Table 2. Case Study Tactics Evident in This Research: Validity and Reliability
Adapted from Yin 2003 p. 34

Design Test	Case Study Tactic	Research Phase
Construct Validity	• Multiple evidence sources—interviews, observations, and document reviews	Data collection
	• Evidence chain	Data collection
	• Informative draft review	Composition
External Validity	• Theoretical base	Research design
Reliability	• Case study protocol	Data collection
	• Case study database	Data collection

CONTRIBUTIONS TO ACADEMIC AND PROFESSIONAL KNOWLEDGE

This research will contribute to the theoretical understanding of the foundational development of information security policy and the policy process, filling a literature gap by

Table 3. Validity in Qualitative Research
Adapted from Creswell and Miller 2000, p. 126 and Creswell 2003, p. 196

Validity in Qualitative Research	
Lens	**Positivist**
Lens of Researcher	Triangulation Data Sources (participants) Theories (IAD, institutional theory) Methods (interviews, observations, and doc reviews) Investigators (debriefing) Disconfirming Evidence Bias Clarification (self-reflection)
Lens of Participant	Member Checking
Lens of Individuals External to Study (reviewers, readers)	Audit Trail Rich description

taking into account both common and IT governance perspectives. Identifying and describing important patterned behaviors in various information security policy environments can provide valuable insights into the fundamental steps in developing comprehensive organizational compliance to vital information security controls. Following this proposed research, further research can identify causal relationships among specific policy process elements and identify possible influencing factors needed for a strong information security program. Most importantly, management theorists will be provided with the tools used in the common governance research field to understand and manage information security challenges.

In addition, practitioners will utilize the best practices suggested in the research to gain new insight early into the policy process by considering multiple variables before the policy development. This understanding will also provide a more efficient means of identifying potential problems that may arise during policy development. As practitioners involved in the policy process better manage the institutional factors that affect information security policy, strong and sustainable policies will be structured.

With a majority of policy research focused on human compliance and implementation after the policy is created, it is time to look at this problem before policy implementation and consider the foundational element in this process—the policy creation itself. Findings from this study can lead to management guidelines and best practices checklists for the construction of solid policies that not only consider the resources but the human element as well. Sustainable policies may lead to improved policy comprehension, policy implementation, and eventually, overall policy compliance.

REFERENCES

Baskerville, R., and Siponen, M. 2002. "An Information Security Meta-Policy for Emergent Organizations," *Logistics Information Management* (15:5/6), pp. 337-346.

Benbasat, I., Goldstein, D. K., and Mead, M. 1987. "The Case Research Strategy in Studies of Information Systems," *MIS Quarterly* (11:3), pp. 369-386.

Box, R. 2010. "Firm Up Your Data Security," *Journal of Accountancy*, (209:6), p. 18.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Quarterly*, (34:3), pp. 523-A7.

Campbell, K., Gordon, L., Loeb, M., and Zhou, L. 2003. "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market," *Journal of Computer Security*, (11:3), p. 431.

Creswell, J.W. 2003. *Research Design: Qualitative, Quantitative, and Mixed Methods*, *Second Edition*. Thousand Oaks, California, USA: Sage Publications.

Creswell, J.W., and Miller, D. 2000. "Determining Validity in Qualitative Inquiry Theory into Practice," (39:3), in *Getting Good Qualitative Data to Improve Educational Practice,* W.G. Tierney and S. Twombly (eds.), Routledge, Summer 2000, pp. 124-130.

D'Archy, J.D., Hovav, A., and Galletta, D. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1), pp. 79-98.

Dhillon, G. 2007. *Principles of Information Systems Security*, Hoboken, NJ: John Wiley & Sons, Inc.

Dinev, T., and Hu, Q. 2007. "The Centrality of Awareness in the Formation of User Behavioral Intention Toward Protective Information Technologies," *Journal of the Association for Information Systems* (8:7), pp. 386-408.

Gall, M.D., Gall, J.P., and Borg, W. 2007. *Educational Research*, *8th Edition*. Massachusetts, USA: Pearson Publishing.

Glesne, C. 2006. *Becoming Qualitative Researchers* (3rd ed.), Boston, MA: Pearson Education Inc.

Guba, E.G., and Lincoln, Y.S. 2005. "Paradigmatic Controversies, Contradictions, and Emerging Confluences," in *The SAGE Handbook of Qualitative Research (*3rd ed.), N.K. Denzin and Y.S. Lincoln (eds.), California, USA: Sage Publications, pp. 191-215.

ISACA. 2011. *COBIT 5*, Rolling Meadows, IL: ISACA.

ISO/IEC: 2005, *Code of Practice for Information Security Management* [Online]. Available from: http://www.iso.org/iso/catalogue_detail?csnumber=39612, [Assessed January 4, 2012].

IT Governance Institute ITGI. 2011. *Global Status Report on Enterprise IT (GEIT)*, Rolling Meadows, IL: ITGI.

Kaplan, B., and Duchon, D. 1988. "Combining Qualitative and Quantitative Methods in Information Systems Research: A Case Study," *MIS Quarterly* (12:4), pp. 571-586.

Leedy, P.D., and Ormrod, J.E. 2001. *Practical Research: Planning and Design, 7th Edition.* New Jersey, USA: Prentice-Hall, Inc.

Madison, M., Frischmann, B., and Strandburg, K. 2008. "Constructing Commons in the Cultural Environment," *Cornell Law Review* (95), pp. 657-709.

March, J.G., and Olsen, J.P. 2009. "Elaborating the 'New Institutionalism'," in *Oxford Handbook of Political Science*, R.E. Goodin, (ed.), New York, NY: Oxford University Press.

NIST 800-12. 1995. *An Introduction to Computer Security: The NIST Handbook* [Online]. Available from: http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf, [Accessed January 4, 2012].

NIST 800-14. 1996. *Generally Accepted Principles and Practices for Securing Information Technology Systems* [Online]. Available from: http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf, [Accessed January 4, 2012].

Nowlin, M.C. 2011. "Theories of the Policy Process: State of the Research and Emerging Trends," *Policy Studies Journal* (39:S1), pp. 41-60.

Office of Management and Budget – OMB 2010. *Fiscal Year 2010 Report to Congress on the Implementation of The Federal Information Security Management Act of 2002*, http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/FY10_FISMA.pdf, [Accessed 21 June 2012].

Ostrom, E. 1990. *Governing the Commons: The Evolution of Institutions for Collective Action*. New York, NY: Cambridge University Press.

Ostrom, E. 2005. *Understanding Institutional Diversity*. Princeton, NJ: Princeton University Press.

Ostrom, E. 2011. "Background on the Institutional Analysis and Development Framework," *Policy Studies Journal* (39:1), pp. 7-27.

Peterson, R. 2004. "Crafting Information Technology Governance," *Information Systems Management* (21:4), pp. 7-22.

Real-Dato, J. 2009. "Mechanisms of Policy Change: A Proposal for a Synthetic Explanatory Framework," *Journal of Comparative Policy Analysis* (11:1), pp. 117-143.

Sabatier, P.A. 1991. "Toward Better Theories of Policy Process," *Political Science and Politics* (24:2), pp. 147-156.

Sabatier, P.A. 2007. "Fostering the Development of Policy Theory," in *Theories of the Policy Process,* P. Sabatier (ed.), Boulder, CO: Westview Press, pp. 321-336.

Schlager, E. 2007. "A Comparison of Frameworks, Theories, and Models of Policy Processes," in *Theories of the Policy Process,* P. Sabatier (ed.), Boulder, CO: Westview Press, pp. 293-319.

Siponen, M., and Willison, R. 2009. "Information Security Management Standards: Problems and Solutions," *Information & Management* (46:5), pp. 267-270.

Siponen, M., and Vance, A. 2010. "Neutralization: New Insights Into the Problem of Employee Information Systems Security Policy Violations," *MIS Quarterly* (34:3), pp. 487-A12.

van Grembergen, W., and de Haes, S. 2008. *Implementing Information Technology Governance: Models, Practices, and Cases*. Hershey, PA: IGI Publishing.

Warkentin, M., Johnston, A.C., and Shropshire, J. 2011. "The Influence of the Informal Social Learning Environment on Information Privacy Policy Compliance Efficacy and Intention," *European Journal of Information Systems* (20:3), pp. 267-284.

Weible, C.M., Heikkila, T., deLeon, P., and Sabatier, P.A. 2012. "Understanding and Influencing the Policy Process," *Policy Sciences* (45:1), pp. 1-21.

Weible, C.M., Sabatier, P.A., Jenkins-Smith, H.C., Nohrstedt, D., Henry, A., and deLeon, P. 2011. "A Quarter Century of the Advocacy Coalition Framework: An Introduction to the Special Issue," *Policy Studies Journal* (39:3), pp. 349-360.

White, G. 2009. "Strategic, Tactical, and Operational Management Security Model," *Journal of Computer Information Systems* (49:3), pp. 71-75.

Whitman, M.E. 2008. "Security Policy," in *Information Security: Policy, Processes and Practices,* D.W. Straub, and S.E. Goodman, Baskerville, R., Armonk, NY, USA: M.E. Sharpe, Inc., pp. 123-151.

Whitman, M.E., and Mattord, H.J. 2010. *Management of Information Security*, Boston, MA: Course Technology Cengage Learning.

Wood, C.C. 2009. *Information Security Policies Made Easy*, Version 11, Houston, TX: Information Shield.

Yin, R.K. 2003. *Case Study Research, Design and Methods*, *3rd Edition*, California, USA: Sage Publications.