

# Information Systems Security: Developing a Stage Theory

---

*Refereed Research Paper*

*Joseph H. Schuessler Ph.D.*

Eastern New Mexico University

College of Business

ENMU Station 49

1500 S Ave K

Portales, New Mexico 88130

575-562-2816

[Joseph.schuessler@enmu.edu](mailto:Joseph.schuessler@enmu.edu)

Chris Taylor, Dean

Information Security and Privacy

Joseph H. Schuessler

# Information Systems Security: Developing a Stage Theory

---

## Abstract

*This is the beginning of a research stream focused on examining information systems research from a stage theory perspective. This paper outline the approach proposed by first giving a detailed look at stage theory in general and then stage theory as it has been applied to information systems specifically. The paper then moves on to discuss a proposed methodology to investigate this phenomenon. The paper then concludes with stating the goals that developing such a model will hopefully fulfill.*

## Introduction

The concept that an organization's Information Systems (IS) Department evolves through stages dates back as to 1969 (Churchill, Kempster and Uretsky 1969). The idea that an organization's IS department has certain characteristics representative of a particular stage suggests that by recognizing key characteristics and how those characteristics are different at different stages, that an organization can "mature" and advance to a stage further down the evolutionary trail. The popularity of using stage theories to explain this evolutionary process is likely due to their intuitive nature (Young 2009, Lucas and Sutton 1977).

Perhaps the best known stage theory as it relates to IS is that put forth by Richard Nolan in which four initial stages were identified: Initiation, Contagion, Control, and Integration (Nolan 1973). While Nolan's stage theory has gone through modifications (Nolan 1973, Gibson and Nolan 1974) and challenges (Benbasat, et al. 1984, King and Kraemer 1984, Lucas and Sutton 1977), the intuitive appeal of understanding how an organization evolves through stages along with characteristics and identifiable steps necessary to advance into more mature stages has served as a driving force with respect to continuing to use stage theories to advance phenomena.

This paper seeks to follow in the footsteps of prior work done regarding stage theory and apply it to the more specific area of IS Security in organizations. Much like the argument of IS in general evolving through stages, it is likely that an organization's security evolves as well as an organization becomes more dependent on their information system and as an organization's investment continues to rise with respect to their information system.

Though relatively little work has been conducted in this specific area or research, one notable exception must be discussed. Young (2009) theorized that an organization's security posture could be associated with one of four prescriptively developed stages. While Young's study did bring a focus on Information Systems Security (ISS) from a stage theory perspective, the prescriptive nature and the lack of variance between respondents with respect to which stages they most identified with made the Young model limited in value.

Much of Young's work built upon the work by King and Teo (1997) in which they prescriptively developed a stage model to describe business and information systems planning. Though appropriate for their model where many of the constructs as they relate to managerial planning are well developed and understood, this approach, it is argued, is not appropriate for examining the various stages in which an organization moves through with respect to their security.

It is argued that a more appropriate approach would be to first develop a stage theory based on descriptive techniques in order to observe the actual stages (assuming they exist), the characteristics of each stage, and the necessary elements necessary to move from one stage to the next. That is the goal of this stream of research; to first develop an understanding of the number and characteristics of stages that exist as it relates to information systems security and then to empirically test the model. This paper's specific goal is to outline an approach to accomplish those stated goals.

## Literature Review

### Stage Theory

Stage theories have been used for years to describe various phenomena. For example, Piaget used stages to describe the development that a child evolves through (Piaget 1950). Marx and Engels (1848) suggested that economic systems evolved through stages from feudalism to communism. By understanding how a phenomena evolves, we can not only anticipate how a phenomena at a lower stage will evolve, but we can potentially affect that evolution in order to make the transitions through stages occur more smoothly and/or potentially more quickly.

As it relates to information systems (IS), considerable research has been conducted describing how an IS department evolves in an organization (Churchill, Kempster and Uretsky 1969, Greiner 1972, Nolan 1973). Perhaps the most notable research conducted using stage theories as it relates to IS has been that conducted by Richard L. Nolan and company (Nolan 1973, Nolan 1979, Nolan 1977, Gibson and Nolan 1974) in which an organization was described as evolving through stages with respect to planning, organizing, and controlling. It was posited that, based on an organization's computer budget, that it would exhibit certain characteristics regarding each of these criteria.

In his initial identification of stages, Nolan (1973) identified four stages which he termed Initiation, Contagion, Control, and Integration in order from least sophisticated to most sophisticated respectively. In the initial stage, the computer system is first introduced into the organization. Few people know how to utilize their new resource and as a result, it often is underutilized. At this stage, little planning, organizing, and controlling activities take place.

Stage two, Contagion, marks the realization that the system can automate and perform many functions and as a result, intense system development occurs. Little planning occurs at this stage. Applications are simply developed hap-hazard in response to user requests with little regard for

integration into other applications/systems. Limited attempts to control and organize occur at this stage.

By stage three, the rapid application development that occurred during stage two has manifested itself as a root cause for a now expensive IS department. These high costs must be brought under control. As a result, controls are put in place in order to regulate application development and avoid the high costs experienced in stage two. Planning starts to become more important in order to more effectively allocate resources to projects deemed necessary by some newly created part of the organization such as a steering committee.

By stage four, Integration, it is realized that overly restrictive controls placed on systems development in stage three do not allow applications to be developed that truly address the needs of users. The realization that a balance needs to be struck between the need for systems development and control functions is recognized. As a result, control functions are relaxed and refined in order to foster appropriate development within the confines of cost restrictions. Refined planning occurs at this stage as does organization of resources.

Nolan argued that at each of these stages, the planning, organizing, and controlling functions of an organization are distinct and that by understanding how an organization evolves, from one stage to another, other organizations could transition from one stage to the next with less disruption. Additionally, by identifying the characteristics that an organization has at a more advanced stage could serve as a model for other organizations wishing to move themselves along the evolutionary model.

In subsequent research, Nolan posited that a fifth stage and sixth stage existed (Nolan 1975). The fifth stage, Data Administration and sixth stage, Maturity, were developed to illustrate an organization's use of data administration and when an organization's application portfolio's data flows mirror the organization's information flows respectively. Consistent with the development of his theory, Nolan

expanded his understanding of the criteria with which an organization could be examined to understand in which stage they existed. Instead of just planning, organizing, and controlling, Nolan expanded those criteria to include application portfolio, data processing organization, data processing planning and control, and user awareness (Nolan 1979). Similar to his previous stage model, Nolan believed that his newer, more complete model could be used to describe an organization and that by understanding the characteristics of organizations at each stage, a better understanding of what it would take to advance to more mature stages would be possible.

It is important to note that in Nolan's conceptualization of stages, organizations simply evolved from one stage to the next. In other words, it was not considered that an organization could either skip from one stage to another without first taking on the characteristics of the stage or stages in between. Likewise, Nolan also did not consider the case where an organization might actually devolve into a lower stage. Miller and Friesen (1984) noted in their study of corporate life cycles that stages could be skipped and that regression from one stage to a prior stage could indeed occur. In the context of an organization's security posture, it suggests that an organization can potentially move from a very early stage of information systems security to a much better developed posture or that they could actually regress to a lower stage representing a less secure organization.

Stage theory is not without its detractors though. Benbasat et al. (1984) in a brief review of Nolan's Stage Theory found little support for the explanatory power of the theory to predict the growth in organizational computing. They noted that while maturity is an intuitively appealing concept, that empirically, it been difficult to measure. They attribute some of this to the dynamic nature of maturity in that our definition of maturity changes over time. This explains the changes in Nolan's model over time to account for additional s-shaped curves requiring the addition of stages five and six. Again, in the context of an organization's IS security, what is representative of a mature organization today could well

be deemed as less than mature a short time later due to advances in technology, strategic changes in the organization's mission, as well as a host of other reasons.

This is not to say that Benbasat et al. (1984) felt Nolan's stage model was totally without merit. To the contrary, they noted that, as it related to Nolan's Stage Theory, it helps to set priorities for managerial attention. Specifically, they noted that hypotheses that generally supported the stage model included hypotheses relating to "senior management, user awareness, and the progression of increasingly formalized management of the IS function" (page 484).

Other detractors from the Nolan stage model included King and Kraemer (1984). They noted the "weak intellectual base" (page 471) upon which the model was based. This "weak intellectual base" occurs due to the model's inability or lack of attention to the larger organizational context in which computing in general occurs. By capturing this larger context, the model would have addressed many of the shortcomings purported by King and Kraemer.

Still another paper in which fault was found with Nolan's work was written by Luca and Sutton (1977). They empirically discovered that time was a better predictor of the growth of computer systems because computer budgets, like most budgets, are usually largely dependent on prior year budgets. As a result, after accounting for inflation and business cycles, the growth in computer budgets reflected a more linear growth pattern than an s-shaped curve.

But they too were quick to point out that stage theories have their place in the literature. Specifically, they point out that due to their descriptive nature that stage models can prove to be very useful. Stage models appeal to managers trying to anticipate managerial problems because of the intuitive nature of stage models.

## Security Posture

As it relates to IS security specifically, stage theories have been attempted in the past (Young 2009) with limited success. Young attempted to prescriptively develop stages and benchmark variables in which an organization's security posture could be assessed. The identification of the number of stages and the development of benchmark variables followed closely the approach by King and Teo (1997). King and Teo developed a stage model to describe the evolution of information systems planning. They, like Young, prescriptively developed the number of stages in their model based not on empirical or even anecdotal evidence of the phenomena in question but rather based on the predominance of the number of stages present on other studies. It is argued that stage theory as applied to IS security is in a formative period (Nolan 1973) and that the approach taken by Young is inappropriate and that a more descriptive approach should be taken initially to identify the stages that an organization moves through with respect to their security.

In regards to the benchmark development, Young (2009) again modeled his stage theory similarly to King and Teo (1997). By adapting the benchmark variable to the IS security domain, Young included the following as his benchmark variables: role of the information security function, role of the information security manager, top management participation in information security planning, user participation in information security planning, performance criteria for the information security function, triggers for information security investments, status of the information security manager, and information security manager participation in business planning. Each of these, it was argued, would be unique to each of the four stages. Each benchmark variable must correlate highly with the other benchmark variables in the same stage (Drury 1983) yet have limited correlation with benchmark variables of other stages (King and Teo 1997).

Though intuitively appealing, each of the benchmark variables put forth by Young (2009) are again argued to be of a prescriptive nature. Rather than including contextual benchmarks as argued by (King

and Kraemer 1984), Young developed benchmarks a priori based on King and Teo's (1997) benchmarks from a significantly different domain where such context is surely different. It is argued that the formative period IS security research in the modern computing era necessitates that a different approach be used in order to produce more meaningful results.

## **Methodology**

Using a grounded theory approach, this research will first identify the number of stages that an organization's security posture goes through and then move on to appropriate benchmark variables. Interviews with 10-15 information systems security professionals will be used to gather data. Benchmark variables as developed by Young (2009) will be used as a way to engage each interviewee and each interviewee will be allowed to discuss their own experiences as it relates to an organization's security posture, evolutionary stages, and appropriate benchmarks.

The interviews will be captured using a digital recorder and then transcribed by the researcher to text files. Each text file will then be imported into MaxQDA, a qualitative data analysis program used to code and categorize as necessary in order to identify patterns across each interview. Patterns that are identified will be used to determine first the existence of stages and then the number of stages if present.

Under the assumption that stages are indeed identified, appropriate benchmark variables will be identified which can be used to illustrate at which stage an organization is given a set of benchmark responses. Various "levels" of each benchmark will be developed that is consistent with findings from the interviews. These "levels" of each benchmark will be used to reflect the differences in the benchmark variable from one stage to the next.

Finally, a stage model will be proposed along with the requisite benchmark variables. A description of each stage and benchmark will be developed to demonstrate the requirements that an organization must possess to be represented within a particular stage in the model. It is this final stage model that will serve as the focus of future research aimed at empirically validating the model

## Results

The results of this research will be a proposed stage theory as it relates to information systems security. As this is research in progress, there are no results to report at this time. However, it is anticipated that approximately 3-6 stages will be identified (King and Teo 1997). In keeping with the tenets of grounded theory, speculation as to the specific number of stages or type of benchmark variables is not presented here.

## Conclusions

The goal of this research is to identify a stage model to explain the stages that an organization moves through with respect to its security posture. It is the initial paper in a line of research that will first, propose the stage theory, to be followed by a paper which will test the theory empirically. In order to test the model empirically, it is anticipated that a survey instrument will be developed in order to obtain data. Following King and Teo (1997), the Del-Test will then be used to assess the validity of the proposed model.

The Del-Test provides for more granular analysis than other techniques commonly applied in stage theory research. The Del-Test allows for one or more benchmarks levels that are not consistent with the rest of the benchmarks for a particular stage to still be considered by effectively weighting the affected benchmark variable(s). For example, if a response appears to be categorized as a stage two respondent, but one of the benchmark variables suggests stage three, then that particular response for that benchmark variable has less impact than it would if it had been consistent with a stage two response but

more impact than had it been a stage four response. This weighting scheme allows more subtle patterns in the data to be determined.

This stream of research will benefit both researchers and practitioners. For researchers, it will shed light on the growth of information systems security within organizations. While much research exists as it relates to information systems security, most of it focuses on technical, social, or socio-technical aspects of security, very little focus has been placed on how organization's mature with respect to information systems security. As a result, there are a number of relevant constructs and relationships that need to be thoroughly vetted.

From the practitioner's perspective, stage models are popular management tools due to their relative ease of use (Young 2009). An easy to use model that explains how information systems security evolves over time will provide managers with a prescriptive tool used to justify future expenditures necessary to migrate the organization to a more advanced stage of information systems security. Additionally, by understanding what it takes to move to more advanced stages, more appropriate purchasing and hiring decisions can be made within the context of understanding the direction that the organization is headed as it relates to future stages for the organization.

<http://isec.sandiego.edu/2011/Default.asp>

## Bibliography

- Benbasat, Izak, Albert S. Dexter, Donald H. Drury, and Robert C. Goldstein. "A Critique of the Stage Hypothesis: Theory and Empirical Evidence." Edited by Gordon Davis. *Communications of the ACM* 27, no. 5 (May 1984): 476-485.
- Churchill, N. C., J. H. Kempster, and M. Uretsky. *Computer Based Information Systems for Management: A Survey*. New York: National Association of Accountants, 1969.
- Drury, D. H. "An Empirical Assessment of the Stages of DP Growth." *MIS Quarterly* 7, no. 2 (1983): 59-70.
- Gibson, Cyrus F., and Richard L. Nolan. "Managing the Four Stages of EDP Growth." *Harvard Business Review*, January-February 1974: 76-88.
- Greiner, R. C. "Evolution and Revolution as Organizations Grow." *Harvard Business Review*, July-August 1972: 37-46.
- King, John Leslie, and Kenneth L. Kraemer. "Evolution and Organizational Informatino Systems: An Assessment of Nolan's Stage Model." *Communications of the ACM* 27, no. 5 (May 1984): 466-175.
- King, W. R., and T. S.H. Teo. "Integration Between Business Planning and Information Systems Planning: Validating a Stage Hypothesis." *Decision Sciences* 28, no. 2 (1997): 279-308.
- Lucas, Henry C., and Jimmy A. Sutton. "The Stage Hypothesis and the S-Curve: Some Contradictory Evidence." *Communications of the ACM* 20, no. 4 (1977): 254-259.
- Marx, Karl, and Friedrich Engels. *The Communist Manifesto*. Communist League, 1848.
- Miller, Danny, and Peter H. Friesen. "A Logitudinal Study of the Corporate Life Cycle." *Management Science* 30, no. 10 (1984): 1161-1183.
- Nolan, Richard L. "Controlling the Cost of Data Services." *Harvard Business Review*, July-August 1977: 114-124.
- . *Management Accounting and Control of Data Processing*. New York: National Association of Accountants, 1977.
- Nolan, Richard L. "Managing the Computer Resource: A Stage Hypothesis." *Communications of the ACM* 16, no. 7 (1973): 399-405.
- Nolan, Richard L. "Managing the Crisis in Data Processing." *Harvard Business Review*, March-April 1979: 115-126.
- . "Organizational Response and Information Technology." Anaheim: AFIPS Natinoal Computer Conference Proceedings, 1978. 517-524.
- Nolan, Richard L. "Plight of the EDP Manager." *Harvard Business Review* 51, no. 3 (May-June 1973): 143-152.

Nolan, Richard L. "Thoughts About the Fifth Stage." *DATABASE* 7, no. 2 (1975): 4-10.

Piaget, Jean. *The Psychology of Intelligence*. London: Routledge and Kegan Paul, 1950.

Young, Randall. "Growth Perspective of Information Security." *Journal of Information Privacy & Security*, October 2009: 51-67.