IS RISK ANALYSIS: A CHAOS THEORETIC PERSPECTIVE

Sumana Sharma, Virginia Commonwealth University, sharmas5@vcu.edu
Gurpreet Dhillon, Virginia Commonwealth University, gdhillon@vcu.edu

ABSTRACT

In this era of rapid globalization information is regarded as a valuable asset. Protection of information through appropriate risk analysis methods and risk management strategies has gained huge momentum. A survey of IS risk management literature reveals that most risk analysis techniques are grounded in the classical probability theory. The scope of the theory is evident from its fundamental assumption that the past is an indication of the future. This makes the theory appropriate for the prediction of known risks, i.e. risks that have already occurred in the past. Nevertheless, the theory has been wrongly applied even to the prediction of unknown risks, i.e. those that have never occurred in the past. We argue that the misapplication of classical probability theory also points to the glaring lack of an alternative theory which in fact addresses the issue of prediction of unknown risks. This paper introduces chaos theory as a means of predicting of such unknown risks to computer based systems, which frequently occur in the IS security landscape.

Keywords: IS Security, Risk Analysis, Chaos theory, Classical probability theory

INTRODUCTION

IS risk analysis is a critical facet of managing security of computer based systems. All researchers of systems security use risk analysis in one form or another [1]. Classical probability theory has traditionally informed risk assessment [2]. An important underlying assumption of the classical probability theory (CPT) is that the past is an indication of the future. This assumption is well suited to the context of predicting the probability of occurrence of known risks and threats, i.e. those that have occurred in the past. The same assumption limits the theory from prediction of unknown risks (that have never occurred in the past) making it impossible to calculate the probability of their reoccurrence in the same or different form in the future. Nevertheless, CPT has been used for predicting unknown risks, i.e. risks that have no past parallel. We argue that the use of CPT to predict unknown risks is not legitimate, because the theory does not purport to deal with unknown risks. Further, it would not be an exaggeration to claim that the absence of any alternative theoretical means to deal with the issue of gaining insight into unknown risks and threats to computer based systems has resulted in continued application of CPT even though it is obvious that prediction of unknown risks is outside the scope of the theory.

Our objectives are twofold. First, we highlight why CPT is inappropriate for prediction of unknown risks. Second, we introduce an alternative theoretical basis in form of chaos theory, as means of predicting ‘unknown’ risks and threats to computer based systems. This paper adopts the definition of risk to a computer based system as a malicious activity likely to result in compromising the confidentiality, integrity and availability of information stored on the system. All other types of risks such as project risks, financial risks, political risks etc (see [3] for a review), are excluded from the scope of the research problem addressed in this paper. It is hoped that considering risks to computer based systems through the use of chaos theory will inform our understanding of predicting risks, specifically the unknown ones, and thereby provide us with the opportunity to better manage them.

The paper is organized into five sections. The first section reviews CPT with an intent to illuminate the issues and challenges associated with the use of the theory in the context of IS security research. The second section reviews the extant IS risk management literature to describe prevalent risk analysis techniques and their theoretical underpinnings. The third section reviews chaos theory and its applications to IS research. The fourth section describes how a chaos theoretic view of risk management could help to address the research problem which cannot be adequately resolved through classical probability theory. The fifth section presents the conclusion and suggests directions for future research.

CLASSICAL PROBABILITY THEORY: TRADITIONAL APPROACH TO IS RISK ANALYSIS – ISSUES AND CHALLENGES

We cannot assume that all problems related to IS can be solved by a single theoretical concept [4]. In the context of risk analysis, the classical probability theory (CPT) has served us well in forecasting future risks and threats based on historic data. It is generally agreed upon that the larger the amount of historic data, the greater is the forecasting accuracy. One of the indispensable building blocks of CPT is the forecaster's ability to measure, as accurately as possible, the probability of occurrence of a certain event. In many cases this probability can then be multiplied by the cost that would be accrued if the event occurred, to calculate a risk score. The risk score could subsequently be used by decision making personnel when attributing resources to combat the range of risks that confront them. Thus application of CPT involves two main steps:

1. Probability of a future event is calculated on the basis of past data.
2. Cost (expenditure) of occurrence of a given event is calculated based on the valuation of the assets involved (affected by) in the event.

A critical assumption underlying the application of CPT to risk analysis is that the forecaster knows what past example to look for. In developing risks analysis techniques, we often neglect this huge assumption and all too simplistically start to dwell on the part that includes calculation of probability and cost related to the occurrence of a given event. These calculations have to be preceded by the simple question: it is the risk of occurrence of 'which' event that we are trying to forecast? If it is an event that has already occurred in the past, we can search our data related past events, look up the event (similar or related event) whose reoccurrence (in the future) we are trying to forecast, and use its probability of occurrence and cost to arrive at (say) a risk score. In other words, we could use the CPT in its purest sense to deal with such a situation. However, the same steps 'cannot' be performed if we do not know what threats we are going to confront in the future. If we use CPT, we might be successful with predicting known threats, but will remain in dark about unknown threats until the time that they actually start staring us in our face.

Use of CPT to forecast risks (e.g. in the field of finance) or events (e.g. in the field of economics) has been met with a lot of success. In fact the credit risk management models of all leading financial services firms utilize the CPT in one or another form to (say) predict the charge off rates for its customers. The application of the CPT theory to IS risk assessment has not been met with the same resounding success. Nevertheless, a large majority of studies in the IS risk literature still utilize the tenets of this theory and its ideas in their risk models and frameworks [3].

It is critical to examine why application of CPT to IS risk analysis has been only limitedly successful whereas its application to areas like finance and economics has been quite successful. In disciplines such as finance and economics, the calculation of probability and cost of occurrence of an event is simplified by the presence of a large amount of historic data as well as the ability to provide at least a somewhat precise valuation of assets affected by a certain event. On the contrary, IS research generally lacks such widely available historic data. Also, the asset in question is 'information', which is intangible making it difficult to assess its worth in monetary terms. or these and other related reasons, use of CPT to conduct risk analysis in IS has been constantly criticized [5].

While lack of historic data and difficulty in determining precise value of information certainly impede the successful application of CPT to IS risk analysis, this is not always the case. This is where we depart from those IS researchers who criticize application of CPT to any stage or form of risk analysis. We believe that CPT serves us well in case of forecasting events (threats) that have occurred in the past. This is because when a threat occurs, the organization inadvertently experiences the effects of the event and the monetary cost associated with the materialization of the event. A careful post-hoc analysis and documentation of relevant data allow the organization to understand the causal factors related to the event. The analysis also helps reveal preventative measures that would inhibit the reoccurrence of the event. If the same event were to reoccur, the organization would be able to improvise on its past experience, increasing the likelihood that the event would be successfully managed. However the challenge lies in the fact that risks are inherently chaotic and therefore generally remain unknown. CPT does not afford us the ability to deal with unknown events which would therefore remain anonymous until the time that they actually materialize leaving little scope for effectively managing them.

LITERATURE REVIEW

Despite the various challenges associated with the use of CPT, it forms the theoretical basis of several risk analysis techniques. This will become more evident in this section where we present a survey of risk management literature. The available risk assessment techniques have been organized into three categories. The first category comprises of techniques based on CPT. The second category comprises of techniques that have been developed as alternatives to classical probability theory. Nevertheless, many of these techniques ultimately utilize the concepts of probability theory. Several others have limited usefulness because of their extremely narrow scope.

Risk Analysis Techniques Based on Classical Probability Theory

Sherer & Alter [3] reviewed 46 articles from the IS literature and summarized the various risk conceptualizations as belonging to three main categories, namely, risk components, risk factors and probability of negative outcomes. They note (p. 33):

> Approximately 1/3 of the studies suggest that risk should be measured as a probability distribution of negative outcomes, often weighted by financial loss. When the IS risk literature deals with probabilities, it tends to show estimates of the probabilities of negative outcomes based on statistical techniques or subjective estimates. Sometimes the negative outcomes are converted to monetary terms and expressed as monetary losses in relation to goals and expectations.

Most risk analysis approaches are grounded in the functionalist paradigm and assert that negative events can be controlled through implementation of appropriate countermeasures [6]. Traditional risk analysis techniques [7,8] treat the issue of risk analysis as something that can be dealt with in a logical and sequential manner. While newer methods or risk analysis have been proposed in the recent IS risk literature, the method of calculating risks as based on the probability of occurrence of a given event has generally remained the same.

Karabacak and Sogukpinar [9] propose ISRAM (Information Security Risk Analysis Method), a quantitative approach that utilizes a paper based survey to analyze security risks of information technologies and allows participation of managers and staff. The risk model underlying ISRAM is inline with the risk formula suggested by NIST [10]. It defines risk as the product of the probability of occurrence of security breach and the consequence of occurrence of security breach. The ISRAM method is initiated by security personnel (those who have knowledge about the given security problem) who discuss the factors affecting a given security problem and assign weights to the factors. These factors are converted to questions and numerical values are assigned to answer choices. Next two risk tables (one for the probability of the risk parameter and one for the consequences of the risk parameter) are prepared which help convert the bulky survey results to meaningful, quantitative and scaled values. These steps are followed by the conducting of the actual survey and analysis of results. This method has a heavy reliance on security personnel (such as, managers) and assumes that these individuals would be able to identify a security problem as well as ‘all’ the factors that could lead to its materialization. Webb [11] propose a six step guideline to ensuring information security. The first step requires security personnel to conduct an information value assessment to identify the various types of valuable information and rank these so that the focus could lie on the most important type. How these could be done, and if it is even possible, has not been discussed.

Straub & Welke [12] advance theory building in risk analysis by proposing a security planning model to help managers cope with systems security risk. The authors believe that assessment of risk requires one to have some idea about the probability of suffering losses and the extent of loss. The managerial guidelines proposed to cope with systems risk require managers to determine unacceptable risks and the countermeasures for these risks. It is not clear how it would be ensured that the managers have determines the complete list of unacceptable risks. The risk analysis approach of Ciechanowicz [13] is also clouded with the same issue.

Risk Analysis Techniques Developed as Alternatives to Classical Probability Theory

Gerber & Solms [14] acknowledge the difficulty in determining the precise value of information and therefore the risks associated with it. The authors pose an interesting question: ‘‘is it possible that the information society has outgrown the approach that traditional risk analysis utilizes? One of the major arguments of the paper is that traditional risk analysis approaches (which were well suited to evaluate risks to tangible IT assets) cannot be extended to evaluate risks to intangible assets such as information. Instead, a holistic approach towards assessing risks to information specific resources should be adopted. The authors categorize current risk analysis methods as belonging to the natural science paradigm, and argue that methods of the social science paradigm also need to be incorporated for proper evaluation of risk.

Despite their criticism of traditional risk analysis approaches (which assume that risk can be quantified), Gerber & Solms [14] still adopt the definition of risk analysis as the sum of risk identification, estimation and evaluation (suggested by Frosdick [15]). Clearly, the same concepts of probability and valuation of assets come into the picture. More importantly, even adoption of the holistic approach proposed by the authors requires valuation of the information resources in the risk analysis stage preceding risk management. This leads to the conclusion that the proposed approach is unable to overcome the issues associated with utilizing the notion of probability theory in evaluating risks.

In order to overcome the fundamental difficulties associated with calculating risks associated with security vulnerabilities, Stewart [16] suggests an alternative approach in form of ‘comparative analysis’ grounded in theory of risk compensation. The authors define comparative analysis as the “ability of an organization to compare a measure of its security to its peers” (p. 364). The author argues that predicting the occurrence of a future attack based on the past is not usually possible because of the lack of reliable data. He states (p. 363):

> The process of attacking and defending computer systems is infinitely reflexive. We modify our defenses in response to attackers who modify their attack in response to our defenses, and so on ad infinitum. This shifting landscape makes any risk calculation extremely difficult because the parameters of the equation are altering rapidly over time. Attempts to model attacker’s actions in an abstract, mathematical way and then to attempt to predict the future actions of attackers based on those models is a problem that is non-trivial and is currently unsolved.

The underlying idea behind the risk compensation theory is that after we introduce a security measure to a system where the current level of security is perceived to already be acceptable, the level of security does not go up, but stays the same. Accordingly the suggestion is to not indulge in a penetrate-and-patch approach, but rather to attack the problem at its roots. This would involve identifying the human and process deficiencies which are generally the cause behind security incidents. The main conclusion drawn by the authors is that predicting the probability of occurrence of future attacks is impossible and hence any effort in this direction is likely to go wasted. It is argued that the comparative analysis technique suggested in the paper is likely to succeed if companies can be encouraged to submit information voluntarily by creating incentives such as participation in comparative analysis would provide them comparative ‘‘rankings’’ on a by-sector basis. While the arguments have been adequately justified through risk compensation theory, it is not very clear if in today’s era when information is considered the greatest asset, a company would be satisfied about its state of security by simply comparing its vulnerability status to that of others. Another important point is that even comparing one’s security vulnerabilities to that of others require an understanding of what constitutes vulnerabilities, i.e. identifying and defining them. This is not always possible because organizations cannot just make a checklist of vulnerabilities, simply because many of these vulnerabilities (especially the ones that have no past parallel) are not readily apparent.

Alternative approaches to quantitative risk management have also been proposed, but not widely adopted due to some form of inherent limitation. Coles & Moulton [17] propose BPIRM or Business Process Information Risk Management a practical approach that relies on an examination of potential losses as the key driver for controls design, rather than a theoretical examination of potential impacts and probabilities of threats and vulnerabilities. They state that the objective of risk management is not to calculate a risk score, but to enable a risk owner to manage risks by getting appropriate controls in place where they are needed (p. 492). However, this method of risk management is entirely focused on business processes and therefore seems to be applicable only to mitigation of business risks.

Labuschagne & Eloff [18] note that current risk management and countermeasure techniques are only able to deal with some of the known threats when infact a bigger problem is posed by threats that have not been identified yet. The authors propose a real time risk analysis method that analysis a communication session in real time to detect threats as they are being launched. While the method overcomes some of the limitations of static risk management methods, it is limited by its ability to only identify threats that emerge as a result of a communication session involving packet data exchange. Further, the method allows us to identify threats when they are on the verge of occurring and not ahead of time. Gerber & Solms [19] propose security requirements analysis as an alternative to the traditional risk analysis when selecting security controls. The authors state that in order to determine appropriate security controls, the amount of security required by the organization needs to be established. There is no guidance provided regarded how this “amount” could be determined. Also the authors state that the security requirements approach includes calculation of risks to the infrastructure. They point out that in many cases organizations can use baseline control manuals to accomplish the risk analysis process; however if they believe that their position is unique they can conduct their own risk analysis. It is apparent that despite its criticism of the traditional risk analysis process, the proposed approach has not been able to escape it or suggest a real alternative.

The application of CPT to risk analysis was criticized by Clements [20] who proposed a different methodology in form of fuzzy set theory. However, Dhillon & Backhouse [6] note that critics have contested the statistical validity of fuzzy metrics. This implies that the problem of prediction of risks, specifically, ‘unknown risks’ still remains unsolved.

It is evident that existing risk analysis approaches are not capable of prediction of unknown risks to computer based systems. A critical flaw underlying these approaches, (both the ones that are based on CPT as well as alternatives to CPT) is their assumption that either organizations are already aware of the risks confronting them or can somehow manage to identify these risks. This assumption is highly misplaced, particularly so, in the current IS security landscape where each risk turns out to be unique and previously unknown. Clearly, there is a strong need for an appropriate alternative theory that affords us the ability to deal with this category of unknown risks. We present chaos theory, as an alternative theory, to deal with this critical and yet unsolved research problem.

CHAOS THEORY & IS RESEARCH

This section describes how a chaos theory view of risk management can position us to predict these risks and threats that have no parallel in the past. A chaos theoretic view is also valuable because risks are inherently chaotic in nature. We first present chaos theory concepts and then the application of chaos theory in the context of Information Systems.

Chaos Theory Concepts

Contrary to what its name might suggest, chaos theory is related to finding (hidden) order in disorder or ‘seemingly’ random data. Gleick [21] refers to chaos as an emerging scientific discipline focusing on the study of non-linear dynamic systems. Non-linear dynamic systems are such systems where small disturbances can have disproportionate (non-linear) effects and whose behavior therefore does not follow predictable and repeatable pathways. Relevant terms and concepts are defined below.

A ***nonlinear system*** (as opposed to a linear system) is a system in which alterations in an initial state need not produce proportional alterations in subsequent states. Such systems do not exhibit any fixed repeatable patterns. Non-linear dynamic systems are inherently unstable and even when stability is reached it may be disturbed by small changes.

Sensitive dependence on initial conditions refers to the fact that a small alteration in the state of a dynamical system will cause subsequent states to differ greatly from the states that would have followed without the alteration. Therefore two otherwise identical chaotic systems with slightly different initial conditions can ultimately reach completely different states, no matter how small the initial difference. The following folklore is often used to explain this concept: "For want of a nail, the shoe was lost; For want of a shoe, the horse was lost; For want of a horse, the rider was lost; For want of a rider, the battle was lost; For want of a battle, the kingdom was lost."

Events are incidents, small or big, immediately apparent or emergent that can amplify small disturbances in a system through a positive feedback and lead to a change in the overall behavior of a system.

A chaotic system can have three ***kinds of equilibrium***: stability, explosive stability and chaotic equilibrium. A system is said to have reached stability when it is controlled by a negative feedback, which brings the system to a new equilibrium position after experiencing all the changes. A system achieves explosive stability when it is driven by a positive feedback which reinforces an initial change to result in an explosive situation. A system is said to be in a chaotic state when there is a simultaneous and unbalanced presence of both positive and negative feedback. This can lead to three situations: ***point attractor*** (when the system eventually reaches equilibrium; ***periodic attractor*** (when the system periodically reaches the equilibrium); or ***strange attractor*** (a state of deterministic chaos when the attractor creates new order in the apparent chaos).

Edge of chaos is the non-equilibrium point at which the system moves to a new strange attractor.

Outcome basin is a subset of the domain of interaction of a system which includes the possible states of a system. The strange attractor iterates within the outcome basin.

Applications of Chaos theory to Information Systems

Although chaos theory was founded on the mathematics of non-linear systems, it has found applicability in the area of social science as well [22]. This can be attributed to the fact that the focus of chaos theory lies on nonlinearity, instability and uncertainty, characteristics of the social world that we humans live in. However, the applications of chaos theory to study various aspects of information systems are few and far between. These are described below.

Dhillon & Ward [4] note that the nature of IS and their role within organizations affords them being studied at various levels – chaos theory offers a meta theoretical basis on which to carry out such studies and argue that chaos theory offers a means to understand the nature of information systems in a variety of contexts. They offer three assertions as to why use of chaos theory to study IS is appropriate: First, that the long term future of IS is unpredictable. Second, predicting outcomes of change caused by IS is virtually impossible. Third, the notion that IS success is a function of adaptation to the environment is too simplistic (p. 8).

McBride [23] utilizes chaos theory as an interpretive model for understanding the complex interactions between information systems and their organizational environments. He applies chaos theory concepts to a case study of IS strategy implementation in the UK probation service and explains how concepts such as initial conditions, strange attractors, edge of chaos and bifurcations can be used to develop a meaningful and coherent story that offers insights into the interactions between IS and organizations.

Dhillon & Fabian [24] note that a non-linear relationship exists between technology and organization. They use the concept of a 'dynamic fractal' to describe the non-linear role played by an information system within an organization and use complexity theory to help managers think about the implications of this nonlinearity. Their assertion that "an information systems is not an asset, but an integral part of the process and dynamic capabilities of the organization, both shaping and being shaped by an organization" (p.130) represents a bridge between the mechanist (technology as an artifact) and vitalist (technology as a social construction) conceptualizations of information systems. The authors contend that when managing technology in organizations (which are instances of nonlinear complex systems), managers need to assess whether or not a coherence exists between the technology and the organization and also ensure that the technology co-evolves with the (changing) organization.

The merits of using complexity theory to study information systems has also been highlighted by Merali [25] who states that the classical information systems paradigm (based on general systems theory) is not able to deal with the emergent nature of information systems. She posits complexity theory as a new paradigm to deal with the increased dynamism and uncertainty prevalent in a network economy like that of today. Beeson & Davis [26] also emphasize upon the inadequacy of systems theories to deal with emergence or change and state that because of their emphasis on maintenance of order, systems theories have generally given an impoverished account of change. They note that "although cybernetic and soft system approaches provide richer notions of change, they still view change as way of preserving or improving order in the system, rather than a fundamental feature of the system itself" (p. 180). They use concepts of complexity theory to develop a systems based theory of generalized change management that views change associated with introduction of a new system as widely distributed and emergent across the organization.

APPLICATION OF CHAOS THEORY TO IS RISK ANALYSIS

We posit chaos theory as a means to deal with understanding the previously unknown risks to computer based systems. Researchers have already argued for the suitability of chaos theory to study information systems in organizations [4, 23]. Dhillon & Ward [4] note that information systems within organizations rarely represent an equilibrium state. Seemingly small disturbances during the design and implementation stages can ultimately result in changing the total behavior of the system. We argue that concepts of chaos theory can also be applied to understanding unknown risks to computer based systems.

Unknown risks to computer based systems can manifest themselves in unimagined ways and lead to disastrous consequences. The increasing number of security breaches despite raised awareness of security problems by organizations seems to be indicative of a colossal flaw in the way we conceptualize and deal with threats to computer based systems. The current efforts of organizations are directed at predicting the reoccurrence of a risk that has confronted them in the past. Needless to say, organizational resources are then directed at implementing security countermeasures to deal with these risks. Certainly, utilizing this method of dealing with risks to computer based systems is akin to hugely oversimplifying the true problem, often at the expense of suffering from the outcome of materialization of the impending threat. Hence, our rationale for adoption of a chaos theoretic perspective to deal with heretofore unknown risks to computer based systems.

Burlando [27] argues that chaos theory has a direct application to the risk management process and provides insightful advice and arguments regarding the applicability of chaos theory to risk management in the context of insurance. He states:

> Risk managers must realize that there is an inescapable link between small seemingly innocuous events and large catastrophic results. The intertwining of small scales with larger ones is not a quirk, bad luck or fortuitous. A hidden structure always exists. (p. 57)

The same arguments are applicable to the context of predicting unknown risks and threats to computer based systems. The risks to a computer based system do not materialize in a flick second. They actually emerge upon a period of time. Conducting a post hoc analysis of a security breach or compromising of information stored on a computer based system can reveal the reasons for the manifestation of the risk and its consequences. In other words, we argue that the manifestation of the risk to the computer based system did not happen by chance, rather there must have been a series of perhaps seemingly unrelated events that led to it appearance. Chaos theory affords us the ability to identify and study these events, thereby also providing us with the opportunity to understand their emergence over a period of time.

It is vital to remember that computer based systems are but an instantiation of information systems within an organization. These systems do not operate in isolation with the organization to which they belong, but rather interact with and are shaped by the organization. It follows that the risks to such computer based systems are likely to be shaped by the organizational context, organizational structure, security policies, human functionaries etc that influence the design and implementation of such systems and the security of information sources stored in them. A computer based systems can be at risk due to small changes (say) due to the manner in which human functionaries implement the security procedures outlined in the security policy, by a change in the organizational structure and numerous other events. Ultimately, the continued interaction among some events might eventually result in a massive security breach. Classical probability theory would not be able to explain it, as there would be no past parallel. On the other hand, chaos theory with its insistence on the simple principle that order can be found in disaster will be much better able to explain the anatomy of such an event and how and why it occurred.

The aim of utilizing chaos theory to understanding risks to computer based systems is not to predict the exact state but rather the overall behavior of the system. Chaos theory concepts tell us that long term predictability is a myth and cannot be achieved. Because events in non-linear dynamic systems are constantly interacting and generating newer patterns, we can at best we can make short term predictions regarding the overall behavior of a system. Nevertheless, use of chaos theory allows us to understand risks and threats as they evolve, know what events could lead to certain risks, attach meaning to patterns of behavior and therefore afford us the ability to better manage these risks. Organizations no longer have to be in the dark regarding hitherto unknown risks and threats confronting their computer bases systems, but rather identify them and therefore not only better manage, but also likely even stop their occurrence.

CONCLUSION

Risk analysis, one of the heavily researched areas the IS security discipline is plagued by two issues. One, there is a heavy reliance on using classical probability theory to predict risks and threats, to the extent that it is being wrongly applied to predict even unknown risks and threats which are clearly outside the purview of CPT. Two, there is a glaring lack of an alternative theory which could be used to deal with the issue of predicting unknown risks and threats, i.e. the ones that have no past parallel. This paper posits chaos theory as a means to deal with the category of unknown risks and threats to computer based systems. It is argued that adoption of a chaos theoretic perspective to risk analysis would lend us the ability to deal with the issue of predicting these unknown risks, and thereby also provide us with the ability to better control and manage them.

Future research could use chaos theory concepts to study instances of security breaches in form of case studies to delve into what events eventually led to the manifestation of the risk in form of a security breach. Such post hoc analysis would be difficult to achieve as it is best to observe patterns of behavior of a system as they happen, but would nevertheless provide rich insight into the anatomy of a security breach, forcing us to think in a structured manner about the manner in which a risk evolved from a threat to a reality. Future research could also focus on utilizing chaos theory software to study historic data related to (say) past security breaches to analyze the strange attractors in the system, the strange attractors that led to the edge of chaos, and the overall patterns of behavior of the system ultimately leading to short term predictability regarding the future behavior of the system. Because chaos theory offers us the ability to delve into a system and understand its possible future behavior, it is of extreme relevance to the context of IS security research which is devoid of adequate theoretical means to deal with unknown risks and threats confronting computer based systems.

REFERENCES

1. Baskerville, R. (1991). Risk analysis: An interpretive feasibility tool in justifying information systems security. *European Journal of Information Systems, 1*, 121-130.

2. Courtney, R. (1977). *Security risk analysis in electronic data processing.* Paper presented at the Proceedings of the AFIPS Conference.
3. Sherer, S. A., & Alter, S. A. (2004). Information system risk and risk factors: Are they mostly about information systems? *Communications of the AIS*, *14*(1), 29-64.
4. Dhillon, G., & Ward, J. (2002). Chaos theory as a framework for studying information systems. *Information Resource Management Journal*, *15*(2), 5-13.
5. Pfleeger, C. (1997). *Security in computing.* (2nd ed.): Prentice Hall, Inc.
6. Dhillon, G., & Backhouse, J. (2001). Current directions in is security research: Towards socio-organizational perspectives. *Information Systems Journal*, *11*, 127-153.
7. Fisher, R. (1984). *Information systems security*. Englewood Cliffs, NJ: Prentice Hall.
8. Parker, D. (1981). *Computer security management*. Reston: Reston Publishing.
9. Karabacak, B., & Sogukpinar, I. (2005). ISRAM: Information security risk analysis method. *Computers & Security*, *24*(2), 147-159.
10. NIST. (2001). *(national institute of standards and technology) risk management guide for information technology systems. Special publication 800-30*.
11. Webb, S. (2000). Crimes and misdemeanours: How to protect corporate information in the internet age. *Computers & Security*, *19*(2), 128-132.
12. Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly*, *22*(4), 441-469.
13. Ciechanowicz, Z. (1997). Risk analysis: Requirements, conflicts and problems. *Computers & Security*, *16*(3), 223-232.
14. Gerber, M., & Solms, R. V. (2005). Management of risk in the information age. *Computers & Security*, *24*(1), 16-30.
15. Frosdick, S. (1997). The techniques of risk analysis are insufficient in themselves. *Disaster Prevention and Management*, *6*(3), 165-177.
16. Stewart, A. (2004). On risk: Perception and direction. *Computers & Security*, *23*(5), 362-370.
17. Coles, R. S., & Moulton, R. (2003). Operationalizing it risk management. *Computers & Security*, *22*(6), 487-493.
18. Labuschagne, L., & Eloff, J. H. P. (1998). The use of real-time risk analysis to enable dynamic activation of countermeasures. *Computers & Security*, *17*(4), 347-357.
19. Gerber, M., & Solms, R. v. (2001). From risk analysis to security requirements. *Computers & Security*, *20*, 577-584.
20. Clements, D. P. (1977). Fuzzy ratings for computer security evaluation: University of California, Berkley
21. Gleick, J. (1987). *Chaos: Making a new science*. Abacus, London.
22. Kiel, L. D., & Elliott, E. W. (1997). *Chaos theory in the social sciences*: Perseus Publishing.
23. McBride, N. (2005). Chaos theory as a model for interpreting information systems in organizations. *Information Systems Journal*, *15*(3), 233-254.
24. Dhillon, G., & Fabian, F. (2005). A fractal perspective on competencies necessary for managing information systems. *Internation Journal of Technology Management*, *31*(1/2), 129-139.
25. Merali, Y. (2004). Complexity and information systems. In M. J. & W. L. (Eds.), *Social theory and philosophy of information systems* (pp. 407-446). John Wiley. Chichester, UK.
26. Beeson, I., & Davis, C. (2000). Emergence and accomplishment in organizational change. *Journal of organizational change management*, *13*(2), 178-189.
27. Burlando, T. (1994). Chaos and risk management. *Risk Management*, *41*(4), 54-61.