

# TOWARDS A PROACTIVE MODEL FOR MANAGING *e*-BUSINESS CONTINUITY

Dr. Cretson L. Dalmadge, Winston-Salem State University  
Dr. Roman M. Wong, Barry University, email: [rwong@mail.barry.edu](mailto:rwong@mail.barry.edu)

## ABSTRACT

*For decades information systems managers addressed the need for continuity in through reactive means – under the umbrella of disaster recovery management. In recent years there has been an increase in the thrust to find proactive ways of managing business continuity. In this paper we utilize vulnerability analysis a basis for proactively managing business continuity. Our framework addresses the causes of business discontinuity and models the relationship between these causes, the risk factors of business discontinuity and the negative consequences associated with business discontinuities. We conclude by proposing a method for proactive management of business continuity through management of the risk factors.*

**Key Words:** Business continuity, discontinuity, risk management, enhancers, suppressors

## INTRODUCTION

Information systems continuity management is becoming increasingly important for today's businesses. Lessons learned from disasters in the 1980s and 1990s plus the threat posed by Y2K have motivated managers to increase their focus on business continuity management and planning (4, 16). Further, incidents such as the tragedies of September 11<sup>th</sup> 2001 have revealed the true value of business continuity management (6, 15). The fact is businesses with systems that are designed for continuity are able recover more quickly after major incidents than businesses with systems that are not designed for continuity. In many cases these businesses have been able to remain online during otherwise disastrous incidents (9).

With businesses continuing to increase their reliance of information systems, a tight link is emerging between information systems continuity and business continuity. This is particularly important for eBusinesses since the business frontier linking a business to its customers is effectively an information system. Effective eBusiness continuity management must therefore start with information system continuity management. Early attempts to address the risk of information systems failure addressed the cause from the standpoint of incidents causing component failure. As such factors capable of triggering discontinuities, e.g. floods, tornadoes and fires, were the platform for the analysis. In addition to these, focus was placed on issues such as component failure. Information systems often fail because there is hardware or software failure. An understanding of those factors, capable of triggering discontinuities, was seen as the underlying and modeling information systems discontinuity (13). This level of analysis (often referred to as failure point analysis) has its merits but comes with serious limitations.

The first shortcoming of failure point analysis is that to effectively predict the likelihood of information systems failure one would need to know the likelihood of occurrence of natural

phenomena such as hurricanes in Florida or tornadoes in the Midwest. The quality of the model would be limited by the business continuity manager's ability to accurately predict these phenomena. Second, as the nature of the issues causing discontinuities continue to grow, analysis centered on component failure will be limiting. Today eBusinesses are suffering discontinuity even as their information systems 'continue to run'. An eBusiness suffering a security breach is having a discontinuity even though it has not suffered any component failure. We propose a model that borrows from the biological sciences utilizing risk factors as a means of assessing the vulnerability of an eBusiness. Measurable characteristics of a given eBusiness are analyzed and used as a means of assessing the vulnerability of the business. We further posit that vulnerability assessment effectively serves as the first step to proactively manage business continuity. It allows manager to proactively address weaknesses within the business and its information systems and make the changes needed to facilitate business continuity.

Biological researchers have addressed the relationship between triggers and risk factors for decades. Their works have led to models for managing the risk of diseases and other ailments within humans and other life forms. Arguably the most renowned of these models is the Framingham Heart Study. Early research studied the risk of heart attack from the perspective of activities that triggered heart attack. Extreme physical activities such as mountain climb or even shoveling snow was therefore discouraged for elderly persons for fear that the activities would trigger heart. Recommendations for younger individuals were less reliable. The Framingham Heart Study moved the focus from the triggers of heart attack to factors within the human body that make us susceptible to heart attack. These include cholesterol level, age, body weight, blood pressure, and whether one smokes. Effective analysis of these factors points to our risk of suffering a heart attack. Further, it provides a basis for us to manage/control these risk factors giving us the ability to decrease our risk of suffering a heart attack (8, 10).

The Framingham Heart Study was initiated in 1948 using a group of 2,336 men and 2,873 women - of Framingham's 28000 residents. In 1971 the Framingham pioneers were joined by 5135 of their sons, daughters, sons-in-law and daughters-in-law in a second phase of the study. Today, more than fifty years later, the Framingham Heart Study is credited with unlocking the secrets of the heart and extending the lives of millions of Americans. The researchers confirmed that there are measurable properties of the human body that effectively serves as indicators for the health of the heart. The resulting model allows us to calculate our risk of suffering a heart attack and take proactive measures to protect the health of our hearts (3, 8, 12, 14).

We posit that eBusinesses and their supporting information systems can be analyzed similarly. Information systems have risk factors. Furthermore, these factors are measurable, providing us with the means to effectively assess the vulnerability of information systems and take measure to reduce the risk of eBusiness discontinuity. Building on the established failure points for information systems, we are able to identify factors that point to increased or decreased risks of information systems failure. Variations in load cycle, for example, may cause an eBusinesses to suffer a discontinuity. An analysis of the factors that allow a business to respond more effectively to these changes will provide some risk factors for eBusinesses. Businesses that are highly scalable are less likely to suffer discontinuity than those with low measure of scalability. Similarly analysis of other triggers provides a list of the risk factors of eBusiness discontinuity.

## MODELING EBUSINESS DISCONTINUITY

Figure 1 shows a framework for assessing the risk of eBusiness discontinuity. The relationship between causes of eBusiness discontinuity, the discontinuity itself and the consequence of eBusiness discontinuity is modeled. Emphasis is also placed on those factors that are capable of influencing the likelihood of occurrence of a discontinuity and the factors capable of moderating final consequences of a discontinuity.

All discontinuities have causes. These are the incidents that trigger the discontinuity itself. Hack attack often result in security breaches for eBusinesses. The occurrence of hack attack itself does not necessarily imply that a discontinuity has occurred. The attack simply serves as a trigger, capable of causing discontinuity. Virus infestation is another classic example of a trigger of eBusiness discontinuity. The virus itself may damage computer systems causing discontinuities. In other cases is disrupt the running of an eBusiness by flooding its network with undesired traffic effectively

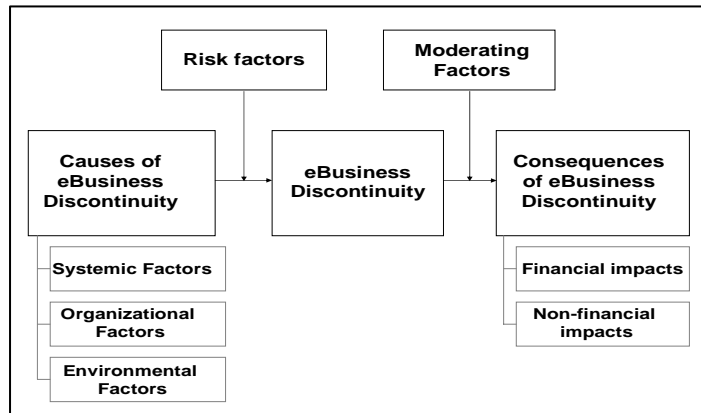


Figure 1: Framework for assessing the vulnerability of eBusinesses

compromising the business' ability to serve its customers. Risk factors regulate the occurrence of discontinuities. In the event of a hack attack, the quality of the security tools used by the eBusiness often dictates the likelihood of a breach. Businesses with weak security or no security tools are expected to suffer far more breaches than those businesses with very strong security measures in place. Analysis of the threat posed by other triggers shows that there are factors within the firms that point to likelihood of the business suffering a discontinuity because of the occurrence of that trigger.

### The Discontinuity

An eBusiness discontinuity occurs when its customers cannot interact with the business in a satisfactory manner. Conversely, eBusiness continuity is maintained as long as the business and its customers can interact satisfactorily. An eBusiness discontinuity may occur in three ways. First, an eBusiness discontinuity has occurred if the eBusiness becomes unavailable. When an eBusiness server goes down without notice, there is naturally a discontinuity. This discontinuity exists as long as the system is unavailable to process customer requests (2, 9). Second, an eBusiness discontinuity has occurred if the eBusiness becomes inaccessible. When the volume of traffic is so high that it is unmanageable, an eBusiness may become inaccessible and thus suffer a discontinuity (5, 7). Third, an eBusiness discontinuity has occurred if the eBusiness fails to deliver adequate quality of service. Even if an eBusiness' systems are available and accessible to its customers, there is a discontinuity if the response time is very slow i.e. below the satisfaction threshold of its customers (11).

### Causes of eBusiness discontinuity

The causes of eBusiness discontinuity are those factors that individually or collectively influence the customers' inability to interact with the business in a satisfactory manner. Causes may be classified along three dimensions: systemic, organizational and environmental (as shown in Figure 1). Systemic factors are those within the eBusinesses information system that are capable of causing discontinuities. Classic examples are hack attacks, system upgrade and component failure. Organizational factors are those factors within the broader organization that are capable of causing discontinuities. These include organizational change and conflict. Environmental factors are those issues within the firm's external environment that can cause discontinuities. These include factors such as environmental change, power failure and earthquakes.

### Triggers versus Risk Factors

Building on the earlier presentation of the adaptation of a biological type model, a distinction is made here between the factors that cause discontinuity. Triggers initiate reactions. They are the single factor that must be present to cause a discontinuity or initiate a series of actions that culminate in a discontinuity. In the case of an email infected with worm viruses, for example, the infected mail triggers initiate a series of actions. The virus itself does not damage the network. Instead, it generates a chain reaction where each recipient unknowingly sends it to others. The end result is network congestion. The congested network is unable to support normal business functions, resulting in an information systems discontinuity.

	Systemic Factors	Organizational Factors	Environmental Factors
Triggers	<ul style="list-style-type: none"> <li>• Component failure</li> <li>• System overload</li> <li>• System maintenance</li> <li>• System upgrade</li> <li>• System replacement</li> <li>• System incompatibility</li> <li>• Date calculations</li> <li>• Other</li> </ul>	<ul style="list-style-type: none"> <li>• Merger, acquisition, divestiture</li> <li>• Reorganization</li> <li>• Leadership change</li> <li>• Retirement, layoff, absence</li> <li>• Power conflict, policy conflict</li> <li>• Decision delay</li> <li>• Load cycle</li> <li>• Other</li> </ul>	<ul style="list-style-type: none"> <li>• Environmental change</li> <li>• Hurricanes</li> <li>• Fire</li> <li>• Flood</li> <li>• Earthquake</li> <li>• Power Failure</li> <li>• Other</li> </ul>
Risk factors	<ul style="list-style-type: none"> <li>• Coupling</li> <li>• Complexity</li> <li>• Reversibility</li> <li>• Maintainability</li> <li>• Connectivity</li> <li>• Human expertise</li> <li>• Design</li> <li>• Scalability</li> <li>• Security</li> <li>• Age</li> <li>• Documentation</li> </ul>	<ul style="list-style-type: none"> <li>• Complexity</li> <li>• Stability</li> <li>• Training</li> <li>• Learning</li> <li>• Knowledge</li> <li>• Cooperation</li> <li>• Monitoring</li> <li>• Adaptability</li> </ul>	<ul style="list-style-type: none"> <li>• Environmental uncertainty</li> <li>• Volatility</li> <li>• Complexity</li> <li>• Exposure</li> <li>• Monitoring</li> </ul>

Figure 2: Causes of eBusiness discontinuity

Risk factors moderate the effects of triggers much like enzymes moderate chemical reactions. This occurs in two ways. First, they may enhance/amplify the effect of the trigger. When a component fails in a tightly coupled system, the resulting discontinuity affects a broad array of subsystems. While coupling itself is desired and sometimes necessary in information systems, tight coupling serves to magnify the scope/effects of the discontinuity.

Second, they may suppress/attenuate the effects of the trigger. Here, the presence of these factors serves to reduce the likelihood and/or scope of the discontinuity. Effective security measures, for example, may prevent a hacker from gaining access to sensitive information even in cases where the hacker gained access to the broader information systems. The presence of these enhancers and suppressors will therefore influence the extent to which triggers translate into discontinuities, much like our cholesterol level points to our likelihood of heart attack. Figure 2 provides a typology for classifying the causes of eBusiness discontinuity. Our analysis of causes of eBusiness discontinuity has identified two dimensions/axes. The first addressed the location of

the causes: i.e. the systemic, organizational and environmental levels. The second addresses the role of the individual factors: i.e. triggers versus risk factors. In Figure 2, we provide a cross tabulation of these two axes. The result is systemic triggers e.g. component failure and system overload; systemic risk factors e.g. coupling, security and maintainability; organizational triggers; organizational risk factors; environmental triggers; and environmental risk factors.

### Consequences of the discontinuity

Discontinuities affect business' ability to satisfactorily serve their customers. Customers are unable to conduct 'business as usual' whenever systems become unavailable or inaccessible.

This creates a potential for loss of revenues for the business. When an airline's web site goes down, it faces the risk of having its customers purchase tickets from competitors. An eBusiness also face the risk of negative impacts of discontinuities when it suffers quality problems. A customer who is unhappy with the quality of service he or she is receiving from an online stock broker will in many cases take his/her business to a competing broker.

The impact of these discontinuities may be analyzed in two ways. First, discontinuities

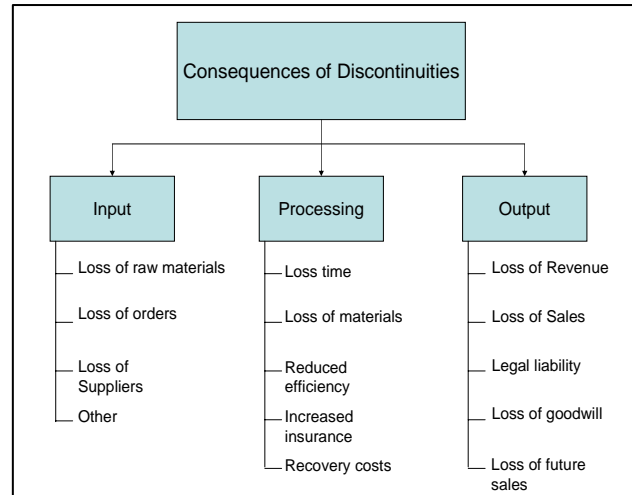


Figure 3: Financial Consequences of eBusiness discontinuity

present the potential for financial loss.

These are quantifiable losses and are classified here in terms of their ability to affect the revenues of the firm. As shown in Figure 3, these losses occur at all levels of operations: input, processing and output levels. Second, many firms suffer non-financial losses. While these losses are indeed capable of affecting the firm's bottom line, they are typically very difficult, if not impossible to quantify. Customer dissatisfaction is an inherent consequence of frequent discontinuities. Dissatisfied customers often leave the business, choosing to do business with their competitors instead. This results in loss of future revenues.

### Moderating Factors:

The process of analyzing the impacts eBusiness discontinuity reveals a non-linear relationship between size of discontinuity and the final consequences. Two firms of similar size - assets and annual revenues - may suffer the same discontinuity (e.g. total shutdown for say four hours) but suffer very different consequences.

Moderating factors dictate the

relationship between potential and actual consequences. Figure 4 shows the taxonomy of moderating factors. As shown, they exist at four levels: industry, business, and product level and

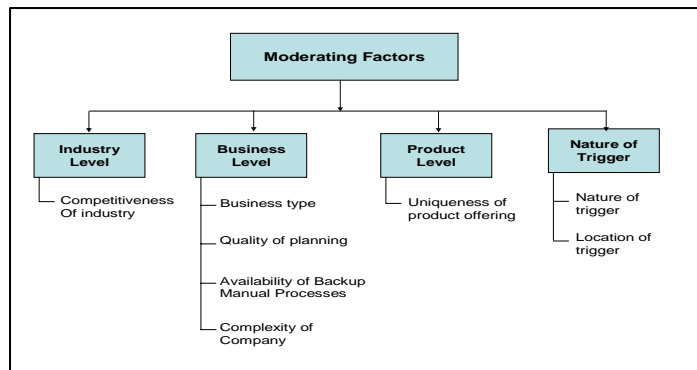


Figure 4: Moderating Factors

the nature of the trigger. Customers are more sympathetic to firms suffering from triggers that are deemed beyond their control for example a tornado. As such, a six hour downtime after a tornado usually has a different impact from a six downtime due to a hack attack. Implying that nature of the trigger does affect the final consequence of a discontinuity.

### Vulnerability Assessment

The broader information systems literature describes risk as a function of two variables: the probability of occurrence of an unfavorable event and the consequence of that event (1). Risk factors serve as indicators of the probability of occurrence of a discontinuity. Moderating factors serve as pointers to the

consequences of eBusiness discontinuity. Analysis and quantification of the two will therefore serve to predict the real vulnerability of an eBusiness. The move to risk factors (and away from failure point analysis) also serves to provide a measurable model for assessing the vulnerability of an eBusiness. While triggers cause eBusiness discontinuity their likelihood of occurrence

is difficult to measure and even immeasurable in many cases. Risk factors are measurable properties of businesses and their information systems. While establish measurement are not presently available for some of the risk factors in Figure 2 it is more feasible to attempt to establish a measurement scale for factors such as scalability, coupling, security and maintainability than to measure the probability of occurrence for triggers such as floods, component failure and environmental change.

Vulnerability analysis involves an examination of each risk factor: measuring its level and applying a weight to account for the relative importance of factors. Security, for example, may be more critical than age as a contributor to the vulnerability of an eBusiness. The aggregate score - from the analysis - points to a level of risk. In this case the scale is developed such that lower scores reflect less vulnerable firms. Similar analysis is performed for the organizational and environmental risk factors. The cumulative score is the vulnerability index of the eBusiness. The model is completed by incorporating the moderating factors into the analysis – thus accounting for the potential consequences of the discontinuity.

Factor	Score [10 point scale]	Weight	Total Points
Coupling	2	0.1	0.2
Complexity	3	0.1	0.3
Reversibility	4	0.15	0.6
Maintainability	4	0.15	0.6
Connectivity	4	0.15	0.6
Human expertise	2	0.2	0.4
Design	2	0.2	0.4
Scalability	5	0.25	1.25
Security	1	0.3	0.3
Age	3	0.156	0.468
Documentation	3	0.2	0.6
<b>Total</b>			<b>5.718</b>

**Figure 4: Sample analysis using systemic risk factors**

### CONCLUSION

We provide a theoretical model for performing vulnerability analysis and as such contribute to the business continuity management. Necessary follow up study is underway to quantify the parameters in the model. The resulting work will serve as the basis for proactively manage business continuity as well as benchmark themselves against industry leaders. The methodology is not limited to eBusinesses. Any business group – irrespective of the type of business – can

adopt a similar approach. Knowledge of failure points provides a basis for development of risk factors. Risk factors then serve as a basis for vulnerability assessment and proactive continuity management

## REFERENCES

1. Boehm, B. W. (1991). "Software Risk Management: Principles and Practices." IEEE Software: 32-41.
2. Boritz, J. E. and J. E. Hunton (2002). "Investigating the Impact of Auditor-Provided Systems Reliability Assurance on Potential Service Recipients." Journal of Information Systems **16**(1): p69, 19p.
3. Brink, S. (1998). "Unlocking the Heart's Secrets." US News and World Report: 58, 8p.
4. Brown, G., M. Fisher, et al. (2000). "Using the Lessons of Y2K to Improve Information Systems Architecture." Communications of the ACM **43**(10): p90, 8p.
5. Chen, E. (1996). IBM no winning medals at Olympics. Electronic News: 2.
6. Dawes, S. S., A. M. Cresswell, et al. (2004). "Learning From Crisis." Social Science Computer Review **22**(1): p52, 15p.
7. Fitzgerald, M. (1996). Who's on First? Editor & Publisher: 13-15.
8. Haynes, S. G. and M. Feinleib (1980). "Women, Work and Coronary Heart Disease: Prospective Findings from the Framingham Heart Study." American Journal of Public Health **70**(2): p133, 9p.
9. Jackson, C. B. (2002). "The Changing Face of Continuity Planning." Information Systems Security **10**(6): p18, 4p.
10. Karasik, D., M. T. Hannan, et al. (2004). "Genetic Contribution to Biological Aging: The Framingham Study." Journals of Gerontology Series A: Biological Sciences & Medical Sciences **59A**(3): p218, 9p.
11. Krause, M. and L. Brown (1996). "Information security in the healthcare industry." Information Systems Security **5**(3): p32, 9p.
12. Lloyd-Jones, D. M., B.-H. Nam, et al. (2004). "Parental Cardiovascular Disease as a Risk Factor for Cardiovascular Disease in Middle-aged Adults: A Prospective Study of Parents and Offspring." JAMA: Journal of the American Medical Association **291**(18): p2204, 8p.
13. Lobel, J. (1980). Risk Analysis in the 1980's. American Federation of Information Processing Societies Proceedings, National Computer Conference.
14. Murabito, J. M., J. M. Byung-Ho Nam, et al. (2004). "Accuracy of Offspring Reports of Parental Cardiovascular Disease History: The Framingham Offspring Study." Annals of Internal Medicine **140**(6): p434, 8p.
15. Musich, P. and E. Koblentz (2003). "Sept. 11 eased blackout." eWeek **20**(34): p13, 3/4p.
16. Stahl, S. (2001). "Lessons Must Be Remembered Forever." InformationWeek(862): p8, 1/2p.
17. Perrow, C., "*Complexity, Coupling and Catastrophe*", In *Normal Accidents*, New York, NY: Basic Books, 1984, pp. 62-100.