A deterministic risk analysis and measurement model for assessing availability and integrity in command and control systems

Madjid Tavana*

Business Systems and Analytics Department,
Lindback Distinguished Chair of Information Systems
and Decision Sciences,
La Salle University,
Philadelphia, PA 19141, USA
and
Business Information Systems Department,
Faculty of Business Administration and Economics,
University of Paderborn, D-33098 Paderborn, Germany
Fax: +1-267-295-2854
Email: tavana@lasalle.edu
*Corresponding author

Dawn A. Trevisani and Thomas A. Clark

Air Force Research Laboratory,
AFRL/RISB,
525 Brooks Road, Rome, NY 13441, USA
Email: Dawn.Trevisani@us.af.mil
Email: Thomas.Clark.27@us.af.mil

Abstract: Military command and control (C2) systems are increasingly challenged by a host of modern problems, namely, internal vulnerabilities and external threats. Several approaches have been suggested in the literature to measure availability and integrity in C2 systems. Despite the importance of developing and maintaining self-protecting and self-healing processes, the simultaneous consideration of availability and integrity has received little attention in the literature. We propose a deterministic quantitative risk analysis and measurement (Q-RAM) framework for C2 systems which is focused on the failure risk induced by internal vulnerabilities and external threats present in the C2 systems. The proposed system allows risk managers to get a comprehensive snapshot of the system availability and integrity, assess the failure risks with the assistance of a multi-factor risk metric, and manage those risks by searching for the best combination of countermeasures, allowing the user to determine the preferred tradeoff between the system's availability and integrity costs.

Keywords: command and control; C2; risk analysis; availability; integrity; countermeasure.

Reference to this paper should be made as follows: Tavana, M., Trevisani, D.A. and Clark, T.A. (2014) 'A deterministic risk analysis and measurement model for assessing availability and integrity in command and control systems', *Int. J. Data Analysis Techniques and Strategies*, Vol. 6, No. 4, pp.327–347.

Biographical notes: Madjid Tavana is a Professor of Business Systems and Analytics and the Lindback Distinguished Chair of Information Systems and Decision Sciences at La Salle University, where he served as the Chairman of the Management Department and Director of the Center for Technology and Management. He is a Distinguished Research Fellow at Kennedy Space Center, Johnson Space Center, Naval Research Laboratory at Stennis Space Center, and Air Force Research Laboratory. He was recently honoured with the prestigious Space Act Award by NASA. He holds a MBA, PMIS, and PhD in Management Information Systems and received his Post-Doctoral Diploma in Strategic Information Systems from the Wharton School at the University of Pennsylvania. He is the Editor-in-Chief of *Decision Analytics*, *International Journal of Applied Decision Sciences*, *International Journal of Management and Decision Making*, *International Journal of Strategic Decision Sciences*, and *International Journal of Enterprise Information Systems*. He has published several books and over one hundred research papers in academic journals such as *Information Sciences*, *Decision Sciences*, *Information Systems*, *Interfaces*, *Annals of Operations Research*, *Advances in Space Research*, *Omega*, *Information and Management*, *Knowledge-Based Systems*, *Expert Systems with Applications*, *European Journal of Operational Research*, *Journal of the Operational Research Society*, *Computers and Operations Research*, *Energy Economics*, *Applied Soft Computing*, and *Energy Policy*.

Dawn Trevisani is a Program Manager/Computer Scientist with the Decision Support Systems Branch at the Air Force Research Laboratory in Rome, New York. She manages modelling and simulation research, experimentation and analysis programmes in response to US Air Force requirements and documented deficiencies. Her focus has been in the area of integrated command and control (C2) architectures, operational level resiliency, decision support systems and course of action generation and assessment. She holds a BS and MS in Computer and Information Science from State University of New York-Institute of Technology at Utica/Rome. She has published in the *International Journal of Information Technology Project Management* and *International Journal of Data Analysis Techniques and Strategies*.

Thomas A. Clark is a Computer Engineer with the Information Directorate at the Air Force Research Laboratory in Rome, New York. He has over 25 years of federal service, holding numerous technical, advisory and management positions in key research areas such as advanced information management and decision support. As an engineer, he has designed, developed and fielded several command and control applications and database designs. As an advisor, he has contributed to and participated in several USAF Chief Scientist and Scientific Advisory Board studies. He holds a BA in Mathematics from SUNY Buffalo, an MS in Computer and Information Science from SUNY Institute of Technology at Utica/Rome, and an MS in Software Development and Management from Rochester Institute of Technology.

1 Introduction

Assuring a secure command and control (C2) system is a major concern in military operations. An enormous amount of effort has been made to develop a wide range of actions to block the attacks on C2 systems. These actions are called countermeasures. Security counter measures help ensure the availability and integrity of the C2 system by preventing and detecting asset losses from security attacks. Prevention ensures that

security breaches do not occur by examining every action and checking its conformance with the security policy before it happens. Detection ensures that sufficient history of the activity in the system is recorded so that a security breach can be detected in a timely fashion after the fact. Countermeasure types can vary considerably. Some countermeasures are designed to limit physical access (e.g., key entry systems, fingerprint scans); some are designed to protect privacy over networks serving the C2system (e.g., firewalls, data encryption), and some are designed to permit recovery if an attack is successful (e.g., backing up important information on a regular basis). Baker and Wallace (2007, p.32) suggest that "researchers should further investigate the benefits of combining various levels of technical, management, and operational controls to achieve true holistic security against a diverse range of present and future risks". However, measuring the holistic financial impact of threats attacking assets is often difficult to measure quantitatively (El-Gayar and Fritz, 2010).

Information systems now monitor and control operations for various infrastructures in government and industry. These systems are often an ad hoc mixture of interdependent components. These interdependencies sometimes allow access for a number of threats that puts these systems at risk. The increasing need for information assurance in government and industry is the direct result of the threat to the government's information infrastructure and the industry's current and future operational capabilities. The concepts of availability and integrity studied here draw heavily from the Department of Defense (DoD) documents. From the DoD perspective, JP 3-13, entitled Joint Doctrine for Information Operations, offers the following widely accepted definition for information assurance:

"Information assurance protects and defends information and information systems by ensuring their availability, integrity, identification and authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities. Information assurance employs technologies and processes such as multilevel security, access controls, secure network servers, and intrusion detection software" [Department of Defense, (1998), III-1].

Information assurance ensures that accurate information and reliable information systems are available to decision-makers when needed. We propose a deterministic quantitative risk analysis and measurement (Q-RAM) framework for information assurance in C2 system which is focused on the failure risk induced by internal vulnerabilities and external threats present in the C2 systems. The proposed model is intended to protect and defend C2 systems by ensuring their availability and integrity. Availability is defined as "assured access by authorized users" and integrity is defined as "protection from unauthorized change" [Armistead, (2004), p.71]. Q-RAM allows risk managers and military planners to get a comprehensive snapshot of the system availability and integrity, assess the failure risks with the assistance of a multi-factor risk metric, and manage those risks by searching for the best combination of countermeasures, allowing the user to determine the preferred tradeoff between the system's availability and integrity costs.

This paper is organised as follows. Section 2 provides a high-level overview of existing approaches to operational risk quantification. Section 3 presents the design and implementation of the system proposed in this study. Section 4 presents a case study and Section 5 offers conclusions and future research directions.

2 Literature review on operational risk quantification

Cyber-risk is the risk involved with a malicious electronic event that causes disruption of operations and monetary loss (Öğüt et al., 2011). Cyber-attacks have a direct impact on the organisations in terms of loss of opportunity cost and organisation's brand equity (Mukhopadhyay et al., 2013). The process approach to operational risk quantification focuses on finding the risk associated with the chain of activities that comprise an operation (Salmela, 2008; Cernauskas and Tarantino, 2009; Dickstein and Flast, 2009). The process approach methods commonly used to quantify operational risks are:

1 causal networks

2 Bayesian belief networks

3 fuzzy logic (Smithson and Paul, 2004).

Causal networks are graphical relationships between the output and input variables in a system. Frank (2002) and Strecker et al. (2011) considered the risks in an organisational hierarchy and proposed a multiple perspective enterprise modelling technique for operational risk assessment. Kokolakis et al. (2000) used the concepts of business process modelling for risk assessment. Salmela (2008) used the concepts of action research and business process modelling for quantifying risks in organisations. Strecker et al. (2011) used the concepts of design science research methodology and proposed a conceptual process modelling method for risk assessment and quantification.

Bayesian belief networks enable reasoning under uncertainty and combine visual representation with Bayesian probability (Krieg, 2001). Guarro (1987) proposed a risk analysis method that used:

1 Bayesian theory for the analysis of security controls

2 the loss potential indicator as the product of the maximum potential loss times the control failure probability to identify the threats that exceeded the organisation's risk threshold

3 cost–benefit analysis to decide on the nature of the controls to be implemented.

The main criticism of this model was that it lacked a holistic organisational view of controls (Baskerville, 1993). Ozeir (1988) considered the following inputs in his Bayesian belief network decision support system:

1 identification of the asset and impact in case of attack

2 mapping of threat to vulnerability

3 exposure distribution and the frequency of occurrence of the attacks.

The outputs of his system included:

1 the risk distribution for each of the attacks

2 the viability of the safeguards to be included for reducing vulnerability of the system

3 a technical analysis report providing detailed information of the security elements to be employed.

Mukhopadhyay et al. (2013) proposed a Bayesian belief network model for cyber vulnerability assessment and expected loss computation. They used the concepts of collective risk modelling theory and computed the premium for a cyber-risk insurer to insure cyber losses. They also proposed a utility-based preferential pricing model that took into account the risk profiles and wealth of the prospective insured firm.

Fuzzy logic is used when some of the system parameters are vague, or have subjective judgments associated with them. Smith and Eloff (2002) proposed using cognitive fuzzy techniques for risk assessment and management in hospitals. They identified the critical patient route in a hospital and assigned risk values for each phase of the patient care system. Ngai and Wat (2005) developed a fuzzy decision support system to assist project managers in identifying potential risk factors and the corresponding risks in information system projects.

Most of the literature on the methods for selection of countermeasures to block or mitigate security attacks is qualitative (Sawik, 2013). For example, Alberts and Dorofee (2002) developed a system called OCTAVE which utilised qualitative information to assess security risk. Egan (2005) developed a checklist in table form to help system planners and decision makers plan a coverage strategy. Bistarelli et al. (2007) proposed a qualitative approach for the selection of security countermeasures for protecting information systems from attacks. They used defense trees and preferences over countermeasure using conditional preference networks to model different security scenarios. Bojanc and Jerman-Blazic (2008) introduced methods for identification of the assets, the threats, and the vulnerabilities of the information systems and a procedure was proposed to enable selection of the optimal investment of the necessary security technology based on the quantification of the values of the protected systems. Chen et al. (2011) discussed current research findings in enterprise risk and security management using mining techniques.

Contrary to qualitative approaches, the literature on quantitative methods for countermeasure selection is very limited (Sawik, 2013). For example, Gupta et al. (2006) designed a system to maximise the coverage of existing vulnerabilities by implementing a set of countermeasures, and thus, minimising the residual vulnerabilities, which were represented as uncovered vulnerabilities. They analysed countermeasure selection in relation to residual vulnerabilities. Deane et al. (2009) developed a linear generalised network flow model for qualifying security risks in the supply chains. They showed how to find solutions for optimal risk reduction under several definitions of optimality: minimising upstream risk, minimising downstream risk, and minimising global supply chain risk. Rees et al. (2011) proposed a decision support system for calculating the uncertain risk associated with an organisation under cyber-attack as a function of uncertain threat rates, countermeasure costs, and impacts on its assets. They used a genetic algorithm to search for the best combination of countermeasures, allowing the user to determine the preferred trade-offs between the cost of the portfolio and the resulting risks. Rakes et al. (2012) developed an integer programming model for optimally choosing a subset of countermeasures to block or mitigate security attacks in the presence of a given threat by examining two different types of scenarios: under expected threat levels and under worst-case levels. They demonstrated the tradeoffs in security planning when expected threats are used to parameterise the model versus worst-case values for threat outcomes. They developed budget-dependent risk curves to demonstrate this trade-off which occurs if decision makers divert budgets away from planning for ordinary risk in an effort to mitigate the effects of potential high-impact

outcomes. Viduto et al. (2012) developed a risk assessment and optimisation model to satisfy organisational security needs by formulating the security countermeasure selection problem as a multi-objective optimisation problem. They constructed a tailored multi-objective tabu search-based heuristic to solve the proposed multi-objective optimisation problem.

3 Q-RAM model

The Q-RAM model is composed of two components: the availability model and the integrity model. Note that the threats to C2 systems seek to adversely affect the availability (through destruction and denial of service) and the integrity (through modification).

3.1 Availability model

Let us consider n assets $a_i (i = 1, 2, \ldots, n)$ and assume $c'_{ij}\left(i = 1,2,\ldots,n; j = 1,2,\ldots,m'_i\right)$ are the countermeasures for the availability of Asset i where m'_i represents the number of availability countermeasures for Asset i. Let us further assume that $e'_{ij}\left(i = 1,2,\ldots,n; j = 1,2,\ldots,m'_i\right)$ represents the effectiveness of the availability countermeasure c'_{ij} and $t'_i(i = 1,2,\ldots n)$ represents the number of attacks on availability per year on Asset i. Assuming that the availability countermeasures c'_{ij} are independent for each Asset i, the availability countermeasures allow the following number of successful attacks on availability per year on Asset $i(s'_i)$ as follows:

$$s'_i = t'_i \cdot \left(1 - \prod_{j=1}^{m'_i} e'_{ij}\right); \left(i = 1,2,\ldots,n; j = 1,2,\ldots,m'_i\right) \tag{1}$$

f'_i is defined as the financial impact of each attack on the availability of Asset i. Therefore the total expected financial impact of all attacks on the availability of Asset $i(F'_i)$ can be calculated as:

$$F'_i = f'_i \cdot s'_i; (i = 1,2,\ldots n) \tag{2}$$

We can find the total expected financial impact of all attacks on the availability of all the assets in the C2 system (F') as follows:

$$F' = \sum_{i=1}^{n} F'_i \tag{3}$$

Next, we construct a table for all possible combinations of effective and ineffective availability countermeasures for the n assets. Each availability countermeasure c'_{ij} has two different states: 0 = *effective* and 1 = *ineffective* and are assumed to be independent of each other. Since there are m'_i different availability countermeasures for Asset i and since each availability countermeasure has two different states, there are $2^{m'_i}$

combinations of these availability countermeasures for Asset *i*. The total number of availability scenarios in the C2 system is the product of the number of different combinations for each asset.

Let $c_{ijk}^{'}$ be the availability countermeasure *j* for Asset *i* and the availability scenario *k*′. $c_{ijk}^{'}=0$ if $c_{ij}^{'}$ for the availability scenario *k*′ is *effective* and $c_{ijk}^{'}=1$ if $c_{ij}^{'}$ for the availability scenario *k*′ is *ineffective*. $d_{ijk}^{'}=e_{ij}^{'}$ if the availability countermeasure *j* is *effective* for Asset *i* and the availability scenario *k*′ and $d_{ijk}^{'}=1-e_{ij}^{'}$ if the availability countermeasure *j* is *ineffective* for Asset *i* and the availability scenario *k*′. The probability of the availability scenario *k*′ for Asset $i(p_{ik}^{'})$ and the joint availability probability of the availability scenario *k*′ for *n* different assets $(q_{k}^{'})$ can be found as follows:

$$p_{ik}^{'}=\prod_{j=1}^{m_i^{'}} d_{ijk}^{'}\left(j=1,2,...,m_i^{'}\right) \tag{4}$$

$$q_{k}^{'}=\prod_{i=1}^{n} p_{ik'}^{'}(i=1,2,\ldots,n) \tag{5}$$

Let us define $\hat{F}_{ik'}^{'}$ as the expected financial impact for Asset *i* for the availability scenario *k*′. The expected financial impact for Asset *i* for the availability scenario $k'(\hat{F}_{ik'}^{'})$ is 0 if $c_{ijk'}^{'}=0$ for all $j=1,2,\ldots,m_i^{'}$ and is $\hat{F}_{ik}^{'}=t_i^{'}\cdot f_i^{'}\cdot q_{k'}^{'}$ if at least one $c_{1jk'}^{'}=1$ for $j=1,2,\ldots,m_i^{'}$; where $t_i^{'}$ is the number of attacks on availability on Asset *i* and $f_i^{'}$ is the financial impact of each attack on availability on Asset *i*. The expected financial impact of the availability scenario *k*′ over all the assets can be found as follows:

$$\hat{F}_{k'}^{'}=\sum_{i=1}^{n}\hat{F}_{k'}^{'}. \tag{6}$$

3.2 Integrity model

Integrity is generally understood as the prevention of unauthorised and improper modification of data (Bertino and Sandhu, 2005). However, this definition is not rigorous since the term 'improper' could mean many things (Sandhu, 1993). In order to provide a comprehensive approach, Bertino et al. (2008) defined a set of meaningful requirements by examining various integrity models. They introduced a notion of a metadata template by which various types of metadata related to integrity requirements could be specified. They also presented a flexible integrity control policy specification language that is able to support not only access control policies but also data validation for preserving data integrity. In their integrity assurance system, data validation was carried out based on metadata values including the data sources.

Let us consider the *n* assets $a_i(i = 1, 2,\ldots, n)$ in the C2 system again. Assuming that:

$c_{ij}^{''}\left(i=1,2,\ldots,n;j=1,2,\ldots,m_i^{''}\right)$ counter measures for the integrity of Asset *i* and $m_i^{''}$

$e_{ij}^{''}\left(i=1,2,\ldots,n;j=1,2,\ldots,m_i^{''}\right)$ effectiveness of the integrity countermeasure $c_{ij}^{''}$

where

m_i'' the number of integrity countermeasures.

$t_i''(i=1,2,\ldots,n)$ number of attacks on integrity per year on Asset *i*

f_i'' financial impact of each attack on integrity on Asset *i*.

The integrity countermeasures allow the following number of successful attacks on the integrity per year of Asset $i(s_i'')$ as follows:

$$s_i'' = t_i'' \cdot \left(1 - \prod_{j=1}^{m_i''} e_{ij}''\right); \left(i=1,2,\ldots,n; j=1,2,\ldots,m_i''\right) \tag{7}$$

The total expected financial impact of all attacks on the integrity of Asset $i(F_i'')$ can be calculated as:

$$F_i'' = f_i'' \cdot s_i''; (i=1,2,\ldots,n) \tag{8}$$

The total expected financial impact of all attacks on the integrity of all the assets in the C2 system (F'') is as follows:

$$F'' = \sum_{i=1}^{n} F_i'' \tag{9}$$

Next, we construct a table for all possible combinations of effective and ineffective integrity countermeasures for the *n* assets similar to the process used for the availability countermeasures. Since there are m_i'' different integrity countermeasures for Asset *i* and since each integrity countermeasure c_{ij}'' has two different states (0 = *effective* and 1 = *ineffective*), there are $2^{m_i''}$ combinations of these integrity countermeasures. The total number of integrity scenarios in the C2 system is the product of the number of different combinations for each asset. Assuming that c_{ijk}'' is the integrity countermeasure *j* for Asset *i* and the integrity scenario *k*″, $c_{ijk}'' = 0$ if c_{ij}'' for the integrity scenario *k*″ is *effective* and $c_{ijk}'' = 1$ if c_{ij}'' for the integrity scenario *k*″ is *ineffective* $d_{ijk}'' = e_{ij}''$ if the integrity countermeasure *j* is *effective* for Asset *i* and the integrity scenario *k*″ and $d_{ijk}'' = 1 - e_{ij}''$ if the integrity countermeasure *j* is *ineffective* for Asset *i* and the integrity scenario *k*″.

$$p_{ik}'' = \prod_{j=1}^{m_i''} d_{ijk}'' \left(j=1,2,\ldots,m_i''\right)$$

is the probability of the integrity scenario *k*″ for Asset *i*. The joint integrity probability of the integrity scenario *k*″ for *n* different assets is

$$q_k'' = \prod_{i=1}^{n} p_{ik''} \quad (i=1,2,\ldots,n).$$

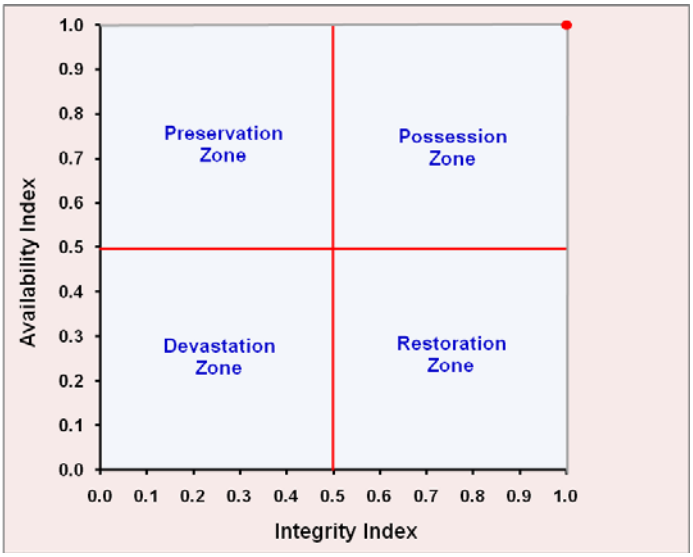
Let us define $\hat{F}''_{ik''}$ as the expected financial impact for Asset i for the integrity scenario k''. The expected financial impact for Asset i for the integrity scenario $k''(\hat{F}''_{ik''})$ is 0 if $c''_{ijk''} = 0$ for all $j = 1, 2, \ldots m''_i$ and is $\hat{F}''_{ik''} = t''_i \cdot f''_i \cdot q''_{k''}$ if at least one $c''_{1jk''} = 1$ for $j = 1, 2, \ldots m''_i$; where t''_i is the number of attacks on integrity on Asset i and f''_i is the financial impact of each attack on integrity on Asset i. The expected financial impact of integrity scenario k'' over all the assets is $\hat{F}''_{k''} = \sum_{i=1}^{n} \hat{F}''_{ik''}$.

Next, we standardise the expected financial impacts of the availability and integrity scenarios for comparative analysis. There are several methods for standardising these expected financial impact figures. We adopt the most frequently used procedure that uses the minimum and maximum scores as scaling points (e.g., Carver, 1991; Malczewski, 1996). Equation (10) is used to calculate the standardised expected financial impact of the availability scenario k' over all assets and equation (11) is used to calculate the standardised expected financial impact of the integrity scenario k'' over all the assets:

$$\hat{F}'_{k'} = \frac{\hat{F}'_{k'} - \hat{F}'^{\min}_{k'}}{\hat{F}'^{\max}_{k'} - \hat{F}'^{\min}_{k'}} \tag{10}$$

$$\hat{F}''_{k''} = \frac{\hat{F}''_{k''} - \hat{F}''^{\min}_{k''}}{\hat{F}''^{\max}_{k''} - \hat{F}''^{\min}_{k''}} \tag{11}$$

Figure 1 A graphical illustration of the proposed model (see online version for colours)



We then plot $\hat{F}'_{k'}$ and $\hat{F}''_{k''}$ on a Cartesian coordinate system. The standardised expected financial impact of the availability scenarios are plotted on the x-axis and the standardised expected financial impact of the integrity scenarios are plotted on the y-axis. The average standardised availability and integrity scores divide this plane into four

quadrants, identified as the possession, preservation, restoration and devastation quadrants. The best point (ideal point) on this grid is point (1,1) where both the availability and integrity scores are at their maximum value (see Figure 1).

- *possession quadrant:* scenarios or assets in this quadrant have above average availability and integrity
- *preservation quadrant:* scenarios or assets in this quadrant have above average availability and below average integrity
- *restoration quadrant:* scenarios or assets in this quadrant have below average availability and above average integrity
- *devastation quadrant:* scenarios or assets in this quadrant have below average availability and integrity.

Figure 1 could be used to represent multiple assets in a C2 system or multiple time periods in the C2 system for comparative analysis and study.

4 Case study

Let us consider a hypothetical C2 system with two assets (a_1, a_2). The average threat against a_1 (Asset 1) occurs at the rate of 100 attacks per year ($t_1 = 100$) and we have two countermeasures of c_{11} and c_{12} with an effectiveness of 80% and 60% ($e_{11} = 0.8$ and $e_{12} = 0.6$) to counteract these attacks. Since the countermeasures (c_{11} and c_{12}) have an effectiveness of 80% and 60%, they will have an ineffectiveness of 20% and 40% ($1 - e_{11} = 0.2$ and $1 - e_{12} = 0.4$). The expected financial impact of each successful attack on Asset 1 is \$5000 ($f_1 = 5{,}000$).

The average threats against a_2 (Asset 2) occurs at the rate of 50 attacks per year ($t_2 = 50$) and we have three countermeasures of (c_{21}, c_{22} and c_{23}) with an effectiveness of 10%, 30%, and 40% ($e_{21} = 0.1$, $e_{22} = 0.3$, and $e_{23} = 0.4$) to counteract these attacks. Since the countermeasures (c_{21}, c_{22} and c_{23}) have an effectiveness of 10%, 30%, and 40%, they will have an ineffectiveness of 90%, 70%, and 60% ($1 - e_{21} = 0.9$, $1 - e_{22} = 0.3$, and $1 - e_{23} = 0.6$). The expected financial impact of each successful attack on Asset 2 is \$6,000 ($f_2 = 6{,}000$).

There are 32 possible scenarios with regards to availability in this C2 system. Assuming that the effectiveness of the counter measures is independent, each countermeasure has two different states: 1 = effective and 0 = ineffective. Since there are two different countermeasures for Asset 1 and since each countermeasure has two different states, there are $2^2 = 4$ combinations of these countermeasures:

1 countermeasures 1 and 2 both effective

2 countermeasure 1 effective and countermeasure 2 ineffective

3 countermeasure 2 effective and countermeasure 1 ineffective

4 countermeasures 1 and 2 both ineffective.

Similarly, there are $2^3 = 8$ combinations for Asset 2. This results in $2^2 \times 2^3 = 32$ possible scenarios in this system presented in Table 1.

Table 1 The expected financial impact of the availability scenarios

Availability scenario	*Asset 1*		*Asset 2*			*Probability of the availability scenario for Asset 1*	*Probability of the availability scenario for Asset 2*	*Joint probability of the availability scenarios for Asset 1 and Asset 2*	*Expected financial impact of the attack on availability for Asset 1*	*Expected financial impact of the attack on availability for Asset 2*	*Expected financial impact of the availability scenario*
	c_{11}	c_{12}	c_{21}	c_{22}	c_{23}						
1	0	0	0	0	0	0.48	0.012	0.00576	0.00	0.00	0.00
2	1	0	0	0	0	0.12	0.012	0.00144	720.00	0.00	720.00
3	0	1	0	0	0	0.32	0.012	0.00384	1,920.00	0.00	1,920.00
4	0	0	1	0	0	0.48	0.108	0.05184	0.00	15,552.00	15,552.00
5	0	0	0	1	0	0.48	0.028	0.01344	0.00	4,032.00	4,032.00
6	0	0	0	0	1	0.48	0.018	0.00864	0.00	2,592.00	2,592.00
7	1	1	0	0	0	0.08	0.012	0.00096	480.00	0.00	480.00
8	1	0	1	0	0	0.12	0.108	0.01296	6,480.00	3,888.00	10,368.00
9	1	0	0	1	0	0.12	0.028	0.00336	1,680.00	1,008.00	2,688.00
10	1	0	0	0	1	0.12	0.018	0.00216	1,080.00	648.00	1,728.00
11	0	1	1	0	0	0.32	0.108	0.03456	17,280.00	10,368.00	27,648.00
12	0	1	0	1	0	0.32	0.028	0.00896	4,480.00	2,688.00	7,168.00
13	0	1	0	0	1	0.32	0.018	0.00576	2,880.00	1,728.00	4,608.00
14	0	0	1	1	0	0.48	0.252	0.12096	0.00	36,288.00	36,288.00
15	0	0	1	0	1	0.48	0.162	0.07776	0.00	23,328.00	23,328.00
16	0	0	0	1	1	0.48	0.042	0.02016	0.00	6,048.00	6,048.00

Table 1 The expected financial impact of the availability scenarios (continued)

Availability scenario	*Asset 1*		*Asset 2*			*Probability of the availability scenario for Asset 1*	*Probability of the availability scenario for Asset 2*	*Joint probability of the availability scenarios for Asset 1 and Asset 2*	*Expected financial impact of the attack on availability for Asset 1*	*Expected financial impact of the attack on availability for Asset 2*	*Expected financial impact of the availability scenario*
	c_{11}	c_{12}	c_{21}	c_{22}	c_{23}						
17	1	0	0	0	1	0.12	0.018	0.00216	1,080.00	648.00	1,728.00
18	0	1	0	0	1	0.32	0.018	0.00576	2,880.00	1,728.00	4,608.00
19	0	0	1	0	1	0.48	0.162	0.07776	0.00	23,328.00	23,328.00
20	0	0	0	1	1	0.48	0.042	0.02016	0.00	6,048.00	6,048.00
21	1	1	1	0	0	0.08	0.108	0.00864	4,320.00	2,592.00	6,912.00
22	1	0	1	1	0	0.12	0.252	0.03024	15,120.00	9,072.00	24,192.00
23	1	0	0	1	1	0.12	0.042	0.00504	2,520.00	1,512.00	4,032.00
24	0	0	1	1	1	0.48	0.378	0.18144	0.00	54,432.00	54,432.00
25	0	1	0	1	1	0.32	0.042	0.01344	6,720.00	4,032.00	10,752.00
26	0	1	1	1	0	0.32	0.252	0.08064	40,320.00	24,192.00	64,512.00
27	0	1	1	0	1	0.32	0.162	0.05184	25,920.00	15,552.00	41,472.00
28	1	0	1	0	1	0.12	0.162	0.01944	9,720.00	5,832.00	15,552.00
29	1	1	1	1	0	0.08	0.252	0.02016	10,080.00	6,048.00	16,128.00
30	1	0	1	1	1	0.12	0.378	0.04536	22,680.00	13,608.00	36,288.00
31	0	1	1	1	1	0.32	0.378	0.12096	60,480.00	36,288.00	96,768.00
32	1	1	1	1	1	0.08	0.378	0.03024	15,120.00	9,072.00	24,192.00

Consider the 32 scenarios $k(k = 1,2,\ldots, 32)$ given in Table 1. Let c_{ijk} be the countermeasure j for Asset i and scenario k. $c_{ijk} = 0$ if c_{ij} for scenario k is *effective* and $c_{ijk} = 1$ if c_{ij} for scenario k is *ineffective*. This defines the values under the Asset 1 and Asset 2 columns in Table 1. $d_{ijk} = e_{ij}$ if countermeasure j is *effective* for Asset i and scenario $k(i = 1,2,\ldots, n; j = 1,2,\ldots m_i; k = 1,2,\ldots, 32)$ and $dijk = 1 - e_{ij}$ if countermeasure j is *ineffective* for Asset i and scenario $k(i = 1,2,\ldots, n; j = 1,2,\ldots m_i; k = 1,2,\ldots, 32)$.

$$p_{1k} = \prod_{j=1}^{2} d_{1jk}\,(j = 1,2)$$

is the probability of scenario k for Asset 1,

$$p_{2k} = \prod_{j=1}^{3} d_{2jk}\,(j = 1,2,3)$$

is the probability of scenario k for Asset 2; or more generally,

$$p_{ik} = \prod_{j=1}^{m_i} d_{ijk}\,\left(j = 1,2,\ldots,m_i\right)$$

is the probability of scenario k for Asset i. The joint probability of scenario k for Asset 1 and Asset 2 is

$$q_k = \prod_{i=1}^{2} p_{ik}\,(i = 1,2);$$

or more generally,

$$q_k = \prod_{i=1}^{n} p_{ik}\,(i = 1,2,\ldots,n)$$

for n different assets.

Introducing $\hat{F}_{ik}$ as the expected financial impact for Asset 1 for scenario k, $\hat{F}_{1k} = 0$ if $c_{1jk} = 0$ for all j and $\hat{F}_{1k} = t_1 \cdot f_1 \cdot q_k$ if at least one $c_{1jk} = 1$ for $j = 1, 2$. Similarly, $\hat{F}_{2k} = 0$ if $c_{2jk} = 0$ for all j and $\hat{F}_{2k} = t_2 \cdot f_2 \cdot q_k$ if at least one $c_{2jk} = 1$ for $j = 1, 2, 3$. More generally, the expected financial impact for Asset i for scenario $k(\hat{F}_{ik})$ is 0 if $c_{ijk} = 0$ for all $j = 1, 2,\ldots, m_i$ and is $\hat{F}_{ik} = t_i \cdot f_i \cdot q_k$ if at least one $c_{1jk} = 1$ for $j = 1, 2,\ldots, m_i$; where t_i is the number of attacks on Asset i (in our example: $t_1 = 100$ and $t_2 = 50$), f_i is the financial impact of each attack on Asset i (in our example: $f_1 = 5{,}000$ and $f_2 = 6{,}000$), the expected financial impact of scenario k is

$$\hat{F}_k = \hat{F}_{1k} + \hat{F}_{2k};$$

or more generally,

$$\hat{F}_k = \sum_{i=1}^{n} \hat{F}_{ik}.$$

Table 2 The expected financial impact of the integrity scenarios

Availability scenario	*Asset 1*		*Asset 2*			*Probability of the integrity scenario for Asset 1*	*Probability of the integrity scenario for Asset 2*	*Joint probability of the integrity scenarios for Asset 1 and Asset 2*	*Expected financial impact of the attack on integrity attack for Asset 1*	*Expected financial impact of the attack on integrity for Asset 2*	*Expected financial impact of the integrity scenario*
	c_{11}	c_{12}	c_{21}	c_{22}	c_{23}						
1	0	0	0	0	0	0.04	0.28	0.0112	0.00	0.00	0.00
2	1	0	0	0	0	0.16	0.28	0.0448	13,440.00	0.00	13,440.00
3	0	1	0	0	0	0.06	0.28	0.0168	5,040.00	0.00	5,040.00
4	0	0	1	0	0	0.04	0.28	0.0112	3,360.00	0.00	3,360.00
5	0	0	0	1	0	0.04	0.12	0.0048	0.00	1,728.00	1,728.00
6	0	0	0	0	1	0.04	0.42	0.0168	0.00	6,048.00	6,048.00
7	1	1	0	0	0	0.24	0.28	0.0672	20,160.00	0.00	20,160.00
8	1	0	1	0	0	0.16	0.28	0.0448	13,440.00	0.00	13,440.00
9	1	0	0	1	0	0.16	0.12	0.0192	5,760.00	6,912.00	12,672.00
10	1	0	0	0	1	0.16	0.42	0.0672	20,160.00	24,192.00	44,352.00
11	0	1	1	0	0	0.06	0.28	0.0168	5,040.00	0.00	5,040.00
12	0	1	0	1	0	0.06	0.12	0.0072	2,160.00	2,592.00	4,752.00
13	0	1	0	0	1	0.06	0.42	0.0252	7,560.00	9,072.00	16,632.00
14	0	0	1	1	0	0.04	0.12	0.0048	1,440.00	1,728.00	3,168.00
15	0	0	1	0	1	0.04	0.42	0.0168	5,040.00	6,048.00	11,088.00
16	0	0	0	1	1	0.04	0.18	0.0072	0.00	2,592.00	2,592.00

Table 2 The expected financial impact of the integrity scenarios (continued)

Availability scenario	*Asset 1*		*Asset 2*			*Probability of the integrity scenario for Asset 1*	*Probability of the integrity scenario for Asset 2*	*Joint probability of the integrity scenarios for Asset 1 and Asset 2*	*Expected financial impact of the attack on integrity attack for Asset 1*	*Expected financial impact of the attack on integrity for Asset 2*	*Expected financial impact of the integrity scenario*
	c_{11}	c_{12}	c_{21}	c_{22}	c_{23}						
17	1	0	0	0	1	0.16	0.42	0.0672	20,160.00	24,192.00	44,352.00
18	0	1	0	0	1	0.06	0.42	0.0252	7,560.00	9,072.00	16,632.00
19	0	0	1	0	1	0.04	0.42	0.0168	5,040.00	6,048.00	11,088.00
20	0	0	0	1	1	0.04	0.18	0.0072	0.00	2,592.00	2,592.00
21	1	1	1	0	0	0.24	0.28	0.0672	20,160.00	0.00	20,160.00
22	1	0	1	1	0	0.16	0.12	0.0192	5,760.00	6,912.00	12,672.00
23	1	0	0	1	1	0.16	0.18	0.0288	8,640.00	10,368.00	19,008.00
24	0	0	1	1	1	0.04	0.18	0.0072	2,160.00	2,592.00	4,752.00
25	0	1	0	1	1	0.06	0.18	0.0108	3,240.00	3,888.00	7,128.00
26	0	1	1	1	0	0.06	0.12	0.0072	2,160.00	2,592.00	4,752.00
27	0	1	1	0	1	0.06	0.42	0.0252	7,560.00	9,072.00	16,632.00
28	1	0	1	0	1	0.16	0.42	0.0672	20,160.00	24,192.00	44,352.00
29	1	1	1	1	0	0.24	0.12	0.0288	8,640.00	10,368.00	19,008.00
30	1	0	1	1	1	0.16	0.18	0.0288	8,640.00	10,368.00	19,008.00
31	0	1	1	1	1	0.06	0.18	0.0108	3,240.00	3,888.00	7,128.00
32	1	1	1	1	1	0.24	0.18	0.0432	12,960.00	15,552.00	28,512.00

Table 1 presents the expected financial impact (cost) for 32 scenarios consisting of 2 assets where the first asset has 2 countermeasures and the second asset has 3 countermeasures. We consider two basic cases for the computation of the expected financial impact of each of the scenarios for each asset. The first case consists of the scenario when all of the countermeasures are effective for a particular asset. In this case the financial impact of the scenario will be 0. A '0' in an asset column means that the countermeasure for that asset is effective and a '1' means that the countermeasure is ineffective.

The second scenario consists of the case where one of the countermeasures (c_{11}) for Asset 1 is ineffective. In this scenario there will be a non-zero expected financial impact for Asset 1. The probability of this scenario is equal to the joint probability of the scenario for Asset 1 and the scenario for Asset 2 (each scenario consists of the combination of a particular scenario for Asset 1 and a particular scenario for Asset 2). The value of this joint probability is .00144 which is the product of 0.12 (the probability of Scenario 2 for Asset 1) and .012 (the probability of Scenario 2 for Asset 2). All the probabilities are calculated by the formulas given in the model. The expected financial impact of Asset 1 for this scenario is equal to .00144 (the probability of Scenario 2) times 100 (the number of attacks per year on Asset 1) times \$5000 (the cost per attack on Asset 1) which is equal to \$720. Notice that the expected financial impact of this scenario on Asset 2 is equal to 0 since this corresponds to the other case where all the countermeasures are effective. The total expected financial impact of this scenario is equal to \$720 which is the sum of the expected financial impact of Asset 1 and Asset 2 for this scenario.

A relatively high value for the expected financial impact of a particular scenario (such as \$64,512 for Scenario 26 and \$96,768 for Scenario 31) is due to relatively high values for the probabilities of each scenario for each asset. The expected financial impact of a particular scenario reflects both the probability of that scenario and the financial impact of that scenario given that it occurs. The expected financial impact of a given scenario can be interpreted as the amount of potential impact that scenario has on the overall cost or risk. Scenarios with high expected financial impact are the ones that should be avoided. Similarly, we find the expected financial impact of the integrity scenarios presented in Table 2.

Next, we ran a simulation study for one year (52 weeks) and standardised the expected financial impacts of the availability and integrity scenarios presented in Table 1 and Table 2 with equations (10) and (11), respectively. The standardised expected financial impacts of the attacks on the availability and the integrity of Asset 1 and Asset 2 in the C2 system for a one year simulation study are presented in Table 3.

We then plotted the results of the simulation study for 52 weeks in Figure 2. Figure 2 presents a snapshot of the C2 system over a 52 week assessment period. As shown in Table 3 and Figure 2, the C2 system simulated in this study was in the possession state for 24 weeks (46%), the devastation state for 13 weeks (25%), the preservation state for 6 weeks (12%), and the restoration state for 9 weeks (17%).

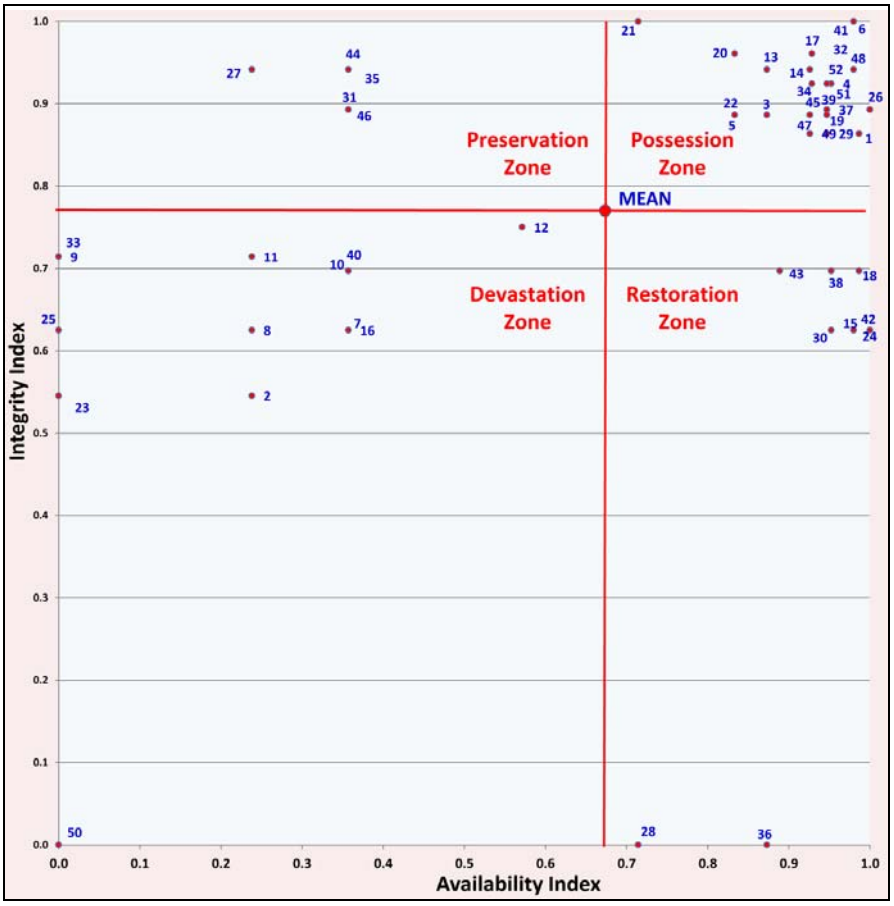
Table 3 Standardised expected financial impacts of the simulation run (see online version for colours)

Week	*Availability*	*Integrity*	*State*
1	0.99	0.86	Possession
2	0.24	0.55	Devastation
3	0.87	0.89	Possession
4	0.95	0.92	Possession
5	0.83	0.89	Possession
6	0.98	1.00	Possession
7	0.36	0.63	Devastation
8	0.24	0.63	Devastation
9	0.00	0.71	Devastation
10	0.36	0.70	Devastation
11	0.24	0.71	Devastation
12	0.57	0.75	Devastation
13	0.87	0.94	Possession
14	0.93	0.94	Possession
15	0.95	0.63	Restoration
16	0.36	0.63	Devastation
17	0.93	0.96	Possession
18	0.99	0.70	Restoration
19	0.95	0.89	Possession
20	0.83	0.96	Possession
21	0.00	0.55	Devastation
22	0.83	0.89	Possession
23	0.71	1.00	Possession
24	1.00	0.63	Restoration
25	0.00	0.63	Devastation
26	1.00	0.89	Possession
27	0.24	0.94	Preservation
28	0.71	0.00	Restoration
29	0.95	0.86	Possession
30	0.95	0.63	Restoration
31	0.36	0.89	Preservation
32	0.24	0.94	Preservation
33	0.00	0.71	Devastation
34	0.93	0.92	Possession
35	0.36	0.94	Preservation
36	0.87	0.00	Restoration
37	0.95	0.89	Possession
38	0.95	0.70	Restoration
39	0.95	0.89	Possession
40	0.36	0.70	Devastation
41	0.98	1.00	Possession

Table 3 Standardised expected financial impacts of the simulation run (continued) (see online version for colours)

Week	*Availability*	*Integrity*	*State*
42	0.98	0.63	Restoration
43	0.89	0.70	Restoration
44	0.36	0.94	Preservation
45	0.93	0.89	Possession
46	0.36	0.89	Preservation
47	0.95	0.89	Possession
48	0.98	0.94	Possession
49	0.93	0.86	Possession
50	0.00	0.00	Devastation
51	0.95	0.92	Possession
52	0.95	0.92	Possession
Average	0.67	0.77	

Figure 2 A snapshot of the C2 system over a 52 week assessment period (see online version for colours)



5 Conclusions and future research directions

The literature describes two broad reasons why inadequate progress has been made on developing information system risk analysis methods. First, most decision makers and managers have no proven and reliable methodology for measuring the effectiveness of their security initiatives (Baker et al., 2007). Second, most decision makers and managers are uncomfortable with having to supply fixed values related to future events which they know to be uncertain (Baker et al., 2007). Various quantitative and qualitative methods such as: annualise loss expectancy (Whitman and Mattord, 2004), the OCTAVE (Alberts and Dorofee, 2002), stochastic dominance (Post and Diltz, 1986), liver more risk analysis methodology (Guarro, 1987), the optimisation of information technology (Badenhorst and Eloff, 1994) and fuzzy sets (Ngai and Wat, 2004; de Ru and Eloff, 1996) are proposed for security risks analysis. Once the security risks have been analysed thoroughly, the next stage involves selecting the best countermeasures for eliminating these risks. Nowadays, organisations apply prevention, detection and recovery-based techniques to eliminate risks (Hamill et al., 2005).

We proposed a deterministic framework for C2 systems which is focused on the failure risk induced by internal vulnerabilities and external threats present in C2 systems. The proposed system provides risk managers with a comprehensive snapshot of the system availability and integrity, the ability to assess the failure risks with the assistance of a multi-factor risk metric, and manage those risks by searching for the best combination of countermeasures, allowing the user to determine the preferred tradeoff between the system's availability and integrity costs.

The proposed framework in this study assumes deterministic parameters in the model. However, these parameters are often uncertain in real-world problems. The source of uncertainty can be vagueness or ambiguity. Vagueness refers to data with lack of clarity and ambiguity refers to data with several overlapping values. While vague data are uncertain because they lack detail or precision, ambiguous data are uncertain because they are subject to multiple interpretations. Fuzzy logic and fuzzy sets can represent vagueness and ambiguity by formalising inaccuracies inherent in human decision-making. Ideas for future research include:

1 considering fuzzy measures for the number of attacks on the availability and the integrity, the number of countermeasures for the availability and integrity attacks, and the effectiveness of the availability and integrity countermeasure in eliminating the threats

2 considering the *attacker's cost* in the financial impact of the attacks on the availability and integrity of the assets

3 assessing the financial impact of each attack on the availability and integrity of the assets in the fuzzy environment.

In this study, we have built upon the groundwork for the consideration of availability and integrity in military C2 systems. We hope that these concepts introduced here will provide inspiration for future research.

Acknowledgements

This research was supported by the U.S. Air Force Research Laboratory grant number FA8750-13-2-0115. The authors would like to thank the anonymous reviewers and the editor for their insightful comments and suggestions.

References

Alberts, C.J. and Dorofee, A.J. (2002) *Managing Information Security Risks: The OCTAVE Approach*, Pearson Education, Inc., Upper Saddle River, New Jersey.

Armistead, L. (Ed.) (2004) *Information Operations: Warfare and the Hard Reality of Soft Power*, Potomac Books, Inc., Washington, D.C.

Badenhorst, K.P. and Eloff, J.H.P. (1994) 'The effect of intrusion detection management methods on the return on investment', *Computers and Security*, Vol. 13, No. 5, pp.411–435.

Baker, W.H. and Wallace, L. (2007) 'Is information security under control?: Investigating quality in information security management', *IEEE Security & Privacy*, Vol. 5, No. 1, pp.36–44.

Baker, W.H., Rees, L.P. and Tippett, P.S. (2007) 'Necessary measures: metric-driven information security risk assessment and decision making', *Communications of the ACM*, Vol. 50, No. 10, pp.101–106.

Baskerville, R.L. (1993) 'Information systems security design methods: implication for information systems development', *ACM Computing Surveys*, Vol. 25, No. 4, pp.375–414.

Bertino, E. and Sandhu, R. (2005) 'Database security – concepts, approaches, and challenges', *IEEE Transaction on Dependable and Secure Computing*, Vol. 2, No. 1, pp.2–19.

Bertino, E., Dai, C., Lim, H.S. and Lin, D. (2008) 'High-assurance integrity techniques for databases', in Gray, A., Jeffery, K.G. and Shao, J. (Eds.): *Sharing Data, Information and Knowledge*, pp.244–256, Springer-Verlag, Berlin, Heidelberg.

Bistarelli, S., Fioravanti, F. and Peretti, P. (2007) 'Using cp-nets as a guide for countermeasure selection', *Proceedings of the 2007 ACM Symposium on Applied Computing*, pp.300–304, Seoul, Korea.

Bojanc, R. and Jerman-Blazic, B. (2008) 'An economic modelling approach to information security risk management', *International Journal of Information Management*, Vol. 28, No. 5, pp.413–422.

Carver, S.J. (1991) 'Integrating multi-criteria evaluation with geographical information systems', *International Journal of Geographical Information Systems*, Vol. 5, No. 3, pp.321–339.

Cernauskas, D. and Tarantino, A. (2009) 'Operational risk management with process control and business process modeling', *The Journal of Operational Risk*, Vol. 4, No. 2, pp.1–22.

Chen, H., Chau, M. and Li, S. (2011) 'Enterprise risk and security management: data, text and web mining', *Decision Support Systems*, Vol. 50, No. 4, pp.649–650.

de Ru, W.G. and Eloff, J.H.P. (1996) 'Risk analysis modelling with the use of fuzzy logic', *Computers and Security*, Vol. 15, No. 3, pp.239–248.

Deane, J.K., Ragsdale, C.T., Rakes, T.R. and Rees, L.P. (2009) 'Managing supply chain risk and disruption from IT security incidents', *Operations Management Research*, Vol. 2, No. 1, pp.4–12.

Department of Defense (1998) *Joint Chiefs of Staff, Joint Publication 3-13*, 9 October, Joint doctrine for Information Operations, Pentagon, Washington.

Dickstein, D.I. and Flast, R.H. (2009) *No Excuses: A Business Process Approach to Managing Operational Risk*, John Willey and Sons Inc., Hoboken, New Jersey.

Egan, M. (2005) *The Executive Guide to Information Security*, Symantec Press, Indianapolis, IN.

El-Gayar, O.F. and Fritz, B.D. (2010) 'A web-based multi-perspective decision support system for information security planning', *Decision Support Systems*, Vol. 50, No. 1, pp.43–54.

Frank, U. (2002) 'Multi-perspective enterprise modeling (MEMO): conceptual framework and modeling languages', *Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS)*, pp.72–82, IEEE Computer Society Washington, DC, USA, Honolulu, HI.

Guarro, S. (1987) 'Principles and procedures of the LRAM approach to information systems risk analysis and management', *Computers and Security*, Vol. 6, No. 6, pp.493–504.

Gupta, M., Rees, J., Chaturvedi, A. and Chi, J. (2006) 'Matching information security vulnerabilities to organizational security profiles: a genetic algorithm approach', *Decision Support Systems*, Vol. 41, No. 3, pp.592–603.

Hamill, J.T., Deckro, R.F. and Kloeber Jr., J.M. (2005) 'Evaluating information assurance strategies', *Decision Support Systems*, Vol. 39, No. 3, pp.463–484.

Kokolakis, S.A., Demopoulos, A.J. and Kiountouzis, E.A. (2000) 'The use of business process modelling in information systems security analysis and design', *Information Management and Computer Security*, Vol. 8, No. 3, pp.107–116.

Krieg, M.L. (2001) *A Tutorial on Bayesian Belief Networks*, Technical Note DSTO-TN-0403, DSTO Electronics and Surveillance Laboratory, Edinburgh, South Australia.

Malczewski, J. (1996) 'A GIS-based approach to multiple criteria group decision making', *International Journal of Geographical Information Systems*, Vol. 10, No. 8, pp.955–971.

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A. and Sadhukhan, S.K. (2013) 'Cyber-risk decision models: to insure IT or not?', *Decision Support Systems* [online] http://dx.doi.org/10.1016/j.dss.2013.04.004 (accessed 13 August 2013).

Ngai, E.W.T. and Wat, F.K.T. (2004) 'Dominance approach to risk analysis of computer systems', *Decision Support Systems*, Vol. 37, No. 4, pp.485–500.

Ngai, E.W.T. and Wat, F.K.T. (2005) 'Fuzzy decision support system for risk analysis in e-commerce development', *Decision Support Systems*, Vol. 40, No. 2, pp.235–255.

Öğüt, H., Raghunathan, S. and Menon, N. (2011) 'Cyber security risk management: public policy implications of correlated risk, imperfect ability to prove loss, and observability of self-protection', *Risk Analysis*, Vol. 31, No. 3, pp.497–512.

Ozeir, W. (1988) 'Risk quantification problems and Bayesian decision support system solutions', *Information Age*, Vol. 11, No. 4, pp.229–234.

Post, G.V. and Diltz, J.D. (1986) 'Dominance approach to risk analysis of computer systems', *MIS Quarterly*, Vol. 10, No. 4, pp.363–375.

Rakes, T.R., Deane, J.K. and Rees, L.P. (2012) 'IT security planning under uncertainty for high-impact events', *Omega: International Journal of Management Science*, Vol. 40, No. 1, pp.79–88.

Rees, L.P., Deane, J.K., Rakes, T.R. and Baker, W.H. (2011) 'Decision support for Cybersecurity risk planning', *Decision Support Systems*, Vol. 51, No. 3, pp.493–505.

Salmela, H. (2008) 'Analyzing business losses caused by information systems risk: a business process analysis approach', *Journal of Information Technology*, Vol. 23, No. 3, pp.185–202.

Sandhu, R. (1993) 'On five definitions of data integrity', *Proceedings of the IFIP WG11.3 Workshop on Database Security*.

Sawik, T. (2013) 'Selection of optimal countermeasure portfolio in IT security planning', *Decision Support Systems*, Vol. 55, No. 1, pp.156–164.

Smith, E. and Eloff, J.H.P. (2002) 'A prototype for assessing information technology risks in health care', *Computers and Security*, Vol. 21, No. 2, pp.266–284.

Smithson, C. and Paul, S. (2004) 'Quantifying operational risk', *Risk*, Vol. 17, No. 7, pp.57–59.

Strecker, S., Heise, D. and Frank, U. (2011) 'RiskM: a multi-perspective modeling method for IT risk assessment', *Information Systems Frontiers*, Vol. 13, No. 4, pp.595–611.

Viduto, V., Maple, C., Huang, W. and Lopez-Perez, D. (2012) 'A novel risk assessment and optimization model for a multi-objective network security countermeasure selection problem', *Decision Support Systems*, Vol. 53, No. 3, pp.599–610.

Whitman, M.E. and Mattord, H.J. (2004) *Management of Information Security*, Course Technology, Thompson, Boston, Massachusetts.