Design Considerations for a Cyber Incident Mission Impact Assessment (CIMIA) Process

Michael R. Grimaila[1], *Senior Member, IEEE,* and Larry W. Fortson[2] and Janet L. Sutton[2]
Center for Cyberspace Research, Air Force Institute of Technology, Wright-Patterson AFB, Ohio 45433, USA
711th Human Performance Wing, Air Force Research Laboratory, Wright-Patterson AFB, Ohio 45433, USA

***Abstract*—Virtually all modern organizations have embedded information systems and networking technologies into their core business processes as a means to increase operational efficiency, improve decision making quality, reduce delays, and/or maximize profit. Unfortunately, this dependence can place the organization's mission at risk when the loss or degradation of the confidentiality, integrity, availability, non-repudiation, or authenticity of a critical information resource or flow occurs. In this paper, we motivate design considerations for an information asset-based, Cyber Incident Mission Impact Assessment (CIMIA) process whose goal is to provide decision makers with timely notification and relevant impact assessment, in terms of mission objectives, from the time an information incident is declared, until the incident is fully remediated.**

Keywords- situational awareness; cyber damage assessment; mission impact assessment

I. Introduction

Information has become the critical asset in the operation and management of virtually all modern organizations [1]. Organizations embed information, communication, and networking technologies into their core mission processes as a means to increase their operational efficiency, exploit automation, reduce response times, improve decision quality, minimize costs, and/or maximize profit [2]-[4]. However, the increasing dependence upon information technology has resulted in an environment where an information incident (e.g., the loss or degradation of the confidentiality, availability, integrity, non-repudiation, and/or authenticity of an information resource or flow) can result in mission failure [5]-[8]. Even when an organization develops and maintains a robust security capability, it is inevitable that the organization will experience an information incident which may result from external attacks, malicious insiders, natural disaster, accidents, and/or equipment failure [3],[8]-[12]. When this occurs, it is important to notify decision makers within organizations whose mission is critically dependent upon the affected information in a timely manner so they can take appropriate contingency measures [8]-[12].

In this paper, we discuss the design considerations for a Cyber Incident Mission Impact Assessment (CIMIA) process, whose purpose is to provide decision makers with timely notification and relevant mission impact estimation, from the instant an information incident is declared, until the incident is fully remediated. While the CIMIA process is being developed for military environments, it is expected to provide utility to any organization that exhibits critical mission-to-information dependencies. The remainder of this paper is structured as follows: In section II, we highlight the importance of incident notification within the military environment. In section III, we discuss the importance of conducting information risk management to provide timely and relevant incident notification. In section IV, we summarize limitations in existing incident notification processes. In section V, we discuss design considerations in the development of the CIMIA process in order to overcome the identified limitations. Finally, in section VI we present our conclusions and make recommendations for future works.

II. The Importance of Notification Following an Information Incident in Miltary Environments

Military organizations have long recognized the benefits and risks of embedding information technology in their mission processes [13]-[15]. Information is continuously collected, processed, analyzed, aggregated, stored, and distributed for multiple purposes including support of situational awareness, operations planning, intelligence, and command decision making [16]. Commanders are often tasked with making critical decisions in short time intervals based upon limited information [17]. As a result, information technologies have significantly improved decision quality by providing commanders the ability to access multiple information resources; obtain frequent updates from these resources; and by enabling correlation among multiple information resources to reduce battlespace uncertainty and improve situational awareness [17]-[19]. The dependency on information technology creates significant mission risks that are often underestimated and may be overlooked [8]-[12].

While all organizations share some common traits, military organizations exhibit unique attributes such as the distributed control of organizational functions across multiple organizational units, time sensitive decision making, and the criticality of consequences that result from bad decision making. In a non-military environment, the consequences are generally expressed in terms of monetary losses. In contrast, in a military environment the consequences may also include physical destruction, injuries, and/or deaths. Since the accuracy, conciseness, and timeliness of the information used in the decision making process dramatically impacts the quality of command decisions, and hence the operational mission outcome; the recognition, quantification, and documentation of information dependencies is essential for the organization to gain a true appreciation of its operational risk [9]-[12]. A failure to identify, document, and understand

This work was supported by a research grant from the Air Force Research Laboratory (F4FBBA9067J001).

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*
13-07-2009

2. REPORT TYPE
Research Conference Paper

3. DATES COVERED *(From - To)*
Oct 2008-Jul 2009

4. TITLE AND SUBTITLE

Design Considerations for a Cyber Incident Mission Impact Assessment (CIMIA) Process

5a. CONTRACT NUMBER
F4FBBA9067J001

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Grimaila, Michael, R.
Fortson, Larry, W.
Sutton, Janet, L.

5d. PROJECT NUMBER
AFIT-2009-ENV-297

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
Center for Cyberspace Research
2950 Hobson Way
Wright-Patterson AFB, OH 45433

8. PERFORMING ORGANIZATION REPORT NUMBER

081025

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Air Force Research Laboratory
Information Operations and Cyberspace Research
Building 248
Wright-Patterson AFB, OH 45433

10. SPONSOR/MONITOR'S ACRONYM(S)

AFRL/RHX

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

2009 International Conference on Security and Management (SAM09)

14. ABSTRACT

Virtually all modern organizations have embedded information systems and networking technologies into their core business processes as a means to increase operational efficiency, improve decision making quality, reduce delays, and/or maximize profit. Unfortunately, this dependence can place the organization's mission at risk when the loss or degradation of the confidentiality, integrity, availability, non-repudiation, or authenticity of a critical information resource or flow occurs. In this paper, we motivate design considerations for an information asset-based, Cyber Incident Mission Impact Assessment (CIMIA) process whose goal is to provide decision makers with timely notification and relevant impact assessment, in terms of mission objectives, from the time an information incident is declared, until the incident is fully remediated.

15. SUBJECT TERMS

Mission assurance; situational awareness; cyber damage assessment; mission impact assessment

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Michael R. Grimaila
a. REPORT U	**b. ABSTRACT** U	**c. THIS PAGE** U	UU	6	**19b. TELEPHONE NUMBER** *(include area code)* 937-255-3636 x4800

critical information dependencies can result in serious consequences as are illustrated in the following hypothetical scenario.

A. The Dangers of Accepting the Status Quo

Consider a hypothetical scenario where a deployed military organization is conducting an operation on foreign soil. One element of the operation requires the periodic delivery of supplies between facilities located in different parts of the country via ground vehicles. The supply company commander uses a logistics database program to manage the resource supply chain for all of the bases in theater. The logistics program is used to maintain a supply inventory for each base, track resource consumption, and schedule resupply missions. The logistics database is stored locally on a server, *Server 1*, within the supply organization and is networked for access by authorized users at other bases. The presence of the database, as well as it criticality, is documented in the certification and accreditation package for *Server 1*. During the operation, a hardware failure occurs in *Server 1* causing a loss of availability of the supply logistics information. The system administration team works to correct the problem, but it takes more than a day to reconstitute the server and restore backups. Based upon experience, one of the system administrators decides to mirror the database to another database server, *Server 2*, located in nearby maintenance unit to insure availability of the database. The system administrator fails to explicitly document this change, so no one else is aware of the mirroring of the logistics database. In the meantime, access to the network is provided to a coalition partner in order to facilitate information sharing on an unrelated mission. A system in the coalition partner's network is compromised, which enables the adversary to escalate their privilege and subsequently breach *Server 2*, the server containing the mirror of the logistics database. The incident is detected by the network security team which notices anomalous encrypted network traffic emanating to and from the database server. An incident is declared and the adversary's access to the database server is terminated. The Incident Response Team (IRT) is dispatched and begins to investigate the incident. The IRT works with the administrators to remediate the incident, conduct a forensic analysis, and notifies all of the documented system users. Despite the fact that the network security team quickly discovered and terminated the breach of *Server 2*, the lack of updating system use documentation results in the convoy commander never being notified of the breach. The following day, one of the convoys listed in the database is ambushed, resulting in a significant loss of life and resources.

While the scenario presented is hypothetical, it illustrates the dire consequences that can result from an organization failing to properly track the status of its critical information resources. While initially there is uncertainty related to the nature of the breach; all of the information contained on the impacted system should be treated as potentially tainted and all organizations that are critically dependent upon the affected information should be notified in an expeditious, relevant, and secure manner. This is the key problem which the CIMIA process seeks to resolve.

III. Information Risk Management

Organizations typically use a risk management process to identify and mitigate information system related risks in order to assure their organizational mission [2],[3],[6],[8]-[12],[20]. Risk management provides a documented, structured, and transparent process to identify critical resources, estimate threats and vulnerabilities that may intersect to cause harm (risks) to critical resources, estimate the likelihood that risks will occur, evaluate tradeoffs between control measures used to mitigate risks, and periodically revisit the analyses as needed. Risk management is comprised of three subordinate processes as shown below in Figure 1: Risk Assessment, Risk Mitigation, and the Evaluation and Assessment process [20].

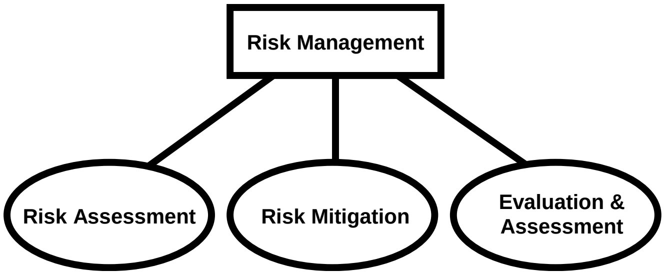

Figure 1. Component Processes of Risk Management [20]

Collectively these processes provide a structured mechanism to identify risks; select preventive, detective, corrective, or reactive control measures to mitigate risks to an acceptable level; and document, communicate, and maintain the analyses so that stakeholders can make informed security resource decisions necessary to insure that organizational resources are protected at a level commensurate with their value.

Risk assessment, the first step of the risk management process, requires the identification of critical organizational resources; estimation of the value they contribute towards accomplishing the organizational mission; enumeration of vulnerabilities that place the resources at risk; identification of threats which may exploit these vulnerabilities; and an estimation of the likelihood that each threat will intersect with a corresponding vulnerability resulting in a loss. Collectively, this information provides the ability to identify mission critical risks, "rack and stack" the risks according to their severity, and develop effective business continuity, contingency, and disaster recovery plans. A key benefit of the risk assessment process is that it requires the organization to explicitly identify and document its critical information resources and articulate how these resources support the organizational mission. Collectively this provides valuable information needed to communicate mission impacts, and potential mission impacts, to decision makers who are critically dependent upon the information in near real time. For this reason, we are primarily focused on the first two elements of the risk assessment process: identification of critical information resources and the estimation of value these resources contribute to the organizational mission.

A. *Information Resource Identification*

Organizations must explicitly identify and document their critical information resources prior to an incident occurring. Documenting critical information resources is important not only to insure they are protected commensurate with their value, but also for the "information accountability" purposes. Identifying critical information resources allows organizations to closely monitor the status of only a small subset of its information resources, allows the identification of transitive information dependencies, and provides the transparency necessary to verify the risk assessment is up-to-date.

B. *Information Resource Valuation*

Organizations must estimate the value that an information resource provides in support of the organizational mission. Value estimation is a very difficult problem due to a variety of reasons [8]-[12], [21]. However, a proper estimation of the information resource value is essential for an accurate risk assessment and is needed to provide relevant notification to decision makers following an information incident. It is important to realize that information valuation is frame of reference dependent, and thus the most accurate estimation of the value will be obtained from those who are most knowledgeable about the use of the information in support of their mission. Accurate valuation requires a formal understanding of the organizational mission, the mission processes, the information processes, and how the given information resource is used in support of the organizational mission.

IV. Barriers to Timely Notification and Relevant Mission Impact Assessment Estimation

In our research, we have identified several technical, organizational, and social barriers that make it difficult to provide timely and relevant incident notification following an information incident [7]-[12]. In this section, we provide a brief summary of each of these barriers to motivate design considerations for the development of the CIMIA process.

A. *The Focus on the Infrastructure*

Existing methods of network defense tend to focus upon the protection of systems and network infrastructure elements, rather than the information stored, processed, and transmitted within the infrastructure. While this abstraction makes it easier to manage security, it misses the primary objective of information security: to assure the security of information. As a consequence, when an information incident occurs, the IRT can not be sure that all downstream users of the affected information are notified in a timely fashion. While this infrastructure-based view greatly simplifies the effort required to assign security controls, it may also lull organizations into a false sense of security due to the belief that a formal risk assessment is unneeded.

B. *The Lack of a Standardized Risk Assessment Process*

While risk assessment is conceptually easy to understand, in practice it is difficult to conduct and maintain in certain environments due to organizational boundaries, the dynamic nature of organizations, the temporal nature of operations, and the inherent subjectivity associated with resource valuation [7]-[12]. In some cases, it may not be possible to maintain an accurate, up-to-date, documented risk profile due to organizational structure, scoping issues, and/or resource constraints.

The lack of standardization in the way that the risk assessment process is conducted reduces the consistency and repeatability of the assessment process and makes it difficult to compare results over time. Without a canonical data representation, it is hard to compare results between and across organizational units. We have found that many organizations fail to properly document their risk assessment findings. Risk assessment is often conducted in an ad-hoc manner. Documentation is seen as a chore and is often the last task completed in a risk assessment.

C. *The Dynamic Nature of Organizations, Missions, and their Information Flows*

Modern organizations are inherently dynamic entities. As the organization changes, its mission changes, or its mission processes change; the information resources the organization requires to support its mission are also likely to change. In this case, the risk assessment process needs to be revisited to insure it provides an accurate assessment of the mission risk. When using existing manual risk assessment processes, this requires an exceptional amount of resources (e.g., effort, personnel, time) which is often deemed as cost prohibitive. As a result, some organizations choose to forgo the risk assessment process in favor of the infrastructure-based or a "best practices" approach at mitigating information system risks. Organizations that fail to maintain current risk assessment processes are unable to understand their true risk profile. Without an explicit understanding of the organization's critical information resources it is difficult to develop effective business continuity, contingency, and disaster recovery plans; difficult to assure information resources are protected commensurate with their value; and virtually impossible to accurately estimate the impact resulting from an information incident when it occurs.

D. *The Lack of Timely and Relevant Incident Notification*

The existing incident notification process is ineffective at providing dependent decision makers with timely and relevant notification following an information incident [8]-[10]. When an information incident is declared, an email is sent to dependent organizations notifying them of the incident. If the notification list is not accurate, all dependent organizational units may not be notified. Even when the proper organizations are notified, the notification may not be passed on to the organizational decision makers. This depends greatly upon the knowledge possessed by the individual who receives the notification. The individual may not understand the potential impact resulting from the incident. As a result, the notification may not be passed on to the organization decision makers who can take appropriate contingency actions to assure the organizational mission.

Another problem is the relevance of the notification. Notification is primarily limited to technical metrics such as the loss of availability and the total man-hours required for the restoration of the system to an operational state. It is often difficult, if not impossible, to translate a low level information incident into its high level mission impact. As a result, the lack of understanding of the impact, or potential impact, resulting from an information incident can lead to poor decision making and the inability to take appropriate contingency actions.

E. *The Lack of Continuity of Knowledge*

When an organization experiences a loss resulting from an information incident, ideally the resulting impacts would be retained and used for understanding future incidents. This is especially true when an information incident occurs because the hidden implications of an incident may not be known until they actually occur. Another consequence of failing to properly document information incidents, and the resulting mission impact, is the lack of an ability to hold organizational units accountable for their actions. In some cases, organizational units will fail to report the true impact due to embarrassment or fear of retribution. As a result, the impact resulting from an information incident may not be disseminated outside of the organizational unit. In contrast, when a flight line accident occurs, there is a significant investigative effort, the responsible individuals are identified, a post-incident briefing is conducted with all involved, remedial action is taken to assure the incident is not repeated, and the lessons learned from the incident are broadcast to all similar organizations.

F. *Security Concerns*

When a risk assessment is conducted, the resources which are most critical to the success of the organizational mission are explicitly identified and documented. As a result, this information becomes a highly sensitive information resource which must be afforded the highest level of protection. If an adversary were able to obtain the results of the risk assessment, they would be able to exploit it and use it to prioritize information resources to maximize the likelihood of disrupting the organizational mission.

V. Design Consideration for a Cyber Incident Mission Impact Assessment Process

In this section, we present design considerations we have identified in the development of a Cyber Incident Mission Impact Assessment (CIMIA) process. Our goal is to overcome identified limitations to provide timely, accurate, secure, and relevant notification from the instant an information incident is declared, until the incident is fully remediated.

A. *An Information Asset Focus*

We believe that a paradigm shift is needed in the way that we identify critical organizational resources. Infrastructure elements are important, but their value is dominated by the value of the information stored, retrieved, processed, and transported through the infrastructure [22]. Information should be the central focus in mission impact assessment because it holds relevance and value as knowledge to decision makers in the organization [22]. Human cognition perceives utility through organization and aggregation of data into usable groupings of contextual relationships that endow the data with “relevance and purpose” [23]. As humans interpret data, it becomes information and meaning is derived [24]. Thus, without the context of the use of information, data have no inherent value [25]. For these reasons, we propose that information, not data, should be the focus when developing a CIMIA process.

An immediate question arises regarding the definition and granularity of an “information resource.” An information resource can be defined as broad as an information system, or as narrow as a specific record within a specific database. If the granularity of an information resource is too fine, there will be too many information resources to be tracked. However, if the granularity of an information resource is too coarse, then the value provided by tracking information will be diminished. This is ongoing research, but we believe that the main value is in the process, which provides information accountability. The granularity of an information resource can be adjusted to meet the needs of the organization. Initially a coarse selection can be chosen, and over time the information resources which require finer granularity can be adjusted.

We must develop standardized and efficient schemes for identifying, valuing, tracking, documenting, and reporting information dependencies in a secure manner [12]. This will provide information resource providers the capability to deterministically identify all those who depend upon their information resources [12]. The identification and valuation of information resources must occur before an incident occurs. This can be accomplished through an information asset-focused risk assessment or other similar information asset profiling techniques [25]-[27].

B. *Improved Techniques for Information Asset Valuation*

Information value determination is difficult as there are both tangible and intangible value components that must be accounted for; the value of information changes over time; and the operational need for information changes over time [11],[12],[25]-[27]. Information valuation is especially difficult in military organizations where the missions are dynamic and ever changing. While many existing information valuation models rely on economic metrics [28], in the military the intangible value of information often far exceeds its tangible economic value. The complexity of context has confounded many attempts at developing models to account for and definitively measure the value of an information asset [29], [30]. This is because information value is always relative to some target goal [31]. Since each organization has its own mission, any impact must be valued in terms of its own frame of reference [8]-[12].

The military possesses a distinct advantage in determining a baseline for the value of its information assets because information is assigned a classification through its uniform system for classifying, safeguarding, and declassifying national security information [32]. However, this only provides a coarse "first cut" for determining the value of information in the context of how it may impact national security and not the organizational mission. In contrast, we are interested in how a compromise of information impacts the organizational mission. Each organization will value their information resource based upon their mission context. When an information resource is valued, the value should contain a description of why the resource is important to the organizational mission. This information can be used to improve the relevance of incident notification by presenting decision makers with an explicit understanding of the value the information provides in support of the mission.

The value of information is a time dependent variable. The mission may require a given resource at one critical point of time in support of its mission, while at other times it may not require it at all. If the resource is inaccessible at the critical point and there is no other source for the information, the result may be inability to complete the mission. Conversely, the resource may be needed continuously throughout the mission. If the resource is inaccessible, the mission may still be able to proceed but at a greater risk of failure or increased harm to friendly forces. Additional work is necessary to identify efficient methods for explicitly representing the value of an information resource as a function of time.

C. *Knowledge Retention*

We believe it is essential to retain actual mission impacts resulting from information incidents in a knowledge base which can be queried to quickly estimate the mission impact resulting from the same, or similar, incidents that have previously occurred. We have found that while organizations may retain records of technical impacts, rarely are the mission impacts retained in a knowledge base. Over time, the retention of the mission impacts can improve the accuracy of mission impact estimation. Effective knowledge management should be at the core of any impact assessment effort [33].

D. *Mission Representation and Mission Impact Estimation*

Alternate mission representations are needed to enable mission-information Situational Awareness (SA). Endsley's Level 2 SA requires a detailed understanding of the significance of the sensed elements in light of the operator's goals [34]. Without a documented understanding of how an information resource supports the organizational mission, efforts at attaining Level 2 SA will be seriously handicapped. Taddaa et al. recognized the need for quantifying the importance of mapping in the Level 3 of their cyber SA model [35]. There is an enormous need to develop new methodologies that assist organizations in creating and maintaining mission mappings. These efforts will require expertise from both the technical and behavioral realms due to the complexity of the problem and the cognitive aspects of criticality quantification.

If we treat information as an asset, we could maintain a state variable for each critical information resource that is maintained by the network security organization. The state of the information resource could be updated in real time by the network security team and the IRT. When an incident occurs, the state of all information resources contained on the affected systems could be changed from the moment the incident occurs until the incident is completely remediated and all investigations are completed. The information resource state variable would represent the belief of five security attributes (e.g., the confidentiality, availability, integrity, non-repudiation, and/or authenticity) in the range of 0-100 for each information resource at any point in time. Associated with each of the five security attributes would be a confidence level in the range 0-100. The state variable could then be fed as input into a mission impact estimation engine maintained at each organization that is dependent upon the affected information. We believe that a mission impact estimation modeling engine can be constructed using a Bayesian network and fuzzy logic that draws upon three primary sources of information: 1) the mission impact assessment estimates collected from subject matter experts prior to the incidents, 2) a historical mission impact database which contains all recorded information incidents and their mission impacts, and 3) explicit mission models which use alternation mission representations (e.g., business process models, information architectures) which can be used to estimate the mission impact based upon modeled dependencies [34].

E. *Secure Notification*

When an information incident occurs, all organizations that are critically dependent upon the affected information must be notified in a timely manner. However, if an adversary is capable of monitoring the notification channel, they can determine which organizations are critically dependent upon the information by attacking a resource and then observing who is notified. For this reason, a pull type of architecture is needed whereby all organizations periodically receive encrypted status information from a central authority [12]. This will prevent an adversary from determining mission criticality by observing the notification process.

VI. CONCLUSIONS

The explosive growth of cyber attacks and the increasing dependency on information technology within military organizations has driven the need to develop efficient methods for communicating mission impact, and potential mission impact, to decision makers following an information incident. The existing methods for incident notification and mission impact assessment are not sufficient at providing accurate, timely, or relevant incident notification in a secure manner. Information should be viewed as an asset and we should focus our efforts on developing technology assisted information asset identification, valuation, tracking, documentation, and reporting capabilities. We believe that our work will enable the development of a near real-time situational awareness tool to provide decision makers with a detailed understanding of mission impact following an information incident in a timely, relevant, and secure manner.

VII. Disclaimer

The views expressed in this paper are those of the authors and do not reflect the official policy or position of the United States Air Force, the Department of Defense, or the U.S. Government.

References

[1] D. Denning, “Information Warfare and Security,” Upper Saddle River, NJ, Pearson, 1999.

[2] M. Abrams, S. Jajodia, and H. Podell eds., “Information Security: An Integrated Collection of Essays,” IEEE Computer Society Press, January 1995.

[3] D.L. Pipkin, “Information Security Protecting the Global Enterprise,” Hewlett-Packard Company, 2000.

[4] E. Anderson, J. Choobineh, J., and M.R. Grimaila, "An Enterprise Level Security Requirements Specification Model," Proceedings of the 38th Annual Hawaii International Conference (HICSS 2005), Jan. 2005, pp. 186-196.

[5] S. Jajodia, P. Ammann, and C.D. McCollum, “Surviving Information Warfare Attacks,” IEEE Computer, Vol. 32, No. 4, pp. 57-63, April 1999.

[6] T. Finne, “Information systems risk management: Key concepts and business processes,” Computers & Security, 19, 3, 234-242, 2000.

[7] R.A. Kemmerer, “Cybersecurity,” IEEE International Conference on Software Engineering (25th). Portland, OR, 2003.

[8] L.W. Fortson and M.R. Grimaila, “Development of a Defensive Cyber Damage Assessment Framework,” Proceedings of the 2007 International Conference on Information Warfare and Security (ICIW 2007); Naval Postgraduate School, Monterey, CA; Mar. 8-9, 2007.

[9] L.W. Fortson, “Towards the Development of a Defensive Cyber Damage and Mission Impact Methodology,” Master's thesis, Air Force Institute of Technology, Department of Systems and Engineering Management, March 2007.

[10] M.R. Grimaila and L.W. Fortson, “Towards an Information Asset-Based Defensive Cyber Damage Assessment Process,” Computational Intelligence in Security and Defense Applications (CISDA 2007), 206-212, April 1-5, 2007.

[11] D. Sorrels, M.R. Grimaila, L.W. Fortson, R.F. Mills, “An Architecture for Cyber Incident Mission Impact Assessment (CIMIA),” Proceedings of the 2008 International Conference on Information Warfare and Security (ICIW 2008), Peter Kiewit Institute, University of Nebraska Omaha, 24-25 April 2008.

[12] M.R. Grimaila, R.F. Mills, and L.W. Fortson, “An Automated Information Asset Tracking Methodology to Enable Timely Cyber Incident Mission Impact Assessment,” Proceedings of the 2008 International Command and Control Research and Technology Symposium (ICCRTS 2008), Bellevue, WA, 17-19 June 2008.

[13] W. Ware, “Security Controls for Computer Systems (U): Report of Defense Science Board Task Force on Computer Security,” The RAND Corporation, Santa Monica, CA; Feb. 1970.

[14] United States General Accounting Office, “Information Security: Computer Attacks at Department of Defense Pose Increasing Risks,” United States General Accounting Office Chapter Report, 22 May 1996.

[15] K. Clark, J. Dawkins, and J. Hale, “Security Risk Metrics: Fusing Enterprise Objectives and Vulnerabilities,” Proceedings of the 2005 IEEE Workshop on Information and Security, United States Military Academy, West Pointm NY, 388-393, 2005.

[16] Joint Chiefs of Staff, “Joint Publication 3-13: Information Operations,” United States Department of Defense, 13 February 2006.

[17] National Defense University Press, “Dominant Battlespace Knowledge,” M. C. Libicki and S. E. Johnson (Ed), October, 1995.

[18] J.G. Diehl and C.E. Sloan, “Battle damage assessment: the ground truth,” Joint Force Quarterly, 2004.

[19] W. Owens, “Lifting the Fog of War,” New York: Farrar, Straus and Giroux, 2000.

[20] G. Stoneburner, A. Goguen, and A. Feringa, “Risk Management Guide for Information Technology Systems,” National Institute of Standards and Technology Special Publication 800-30, 2002.

[21] D. Hellesen, M.R. Grimaila, L.W. Fortson, R.F. Mills, “Information Asset Value Quantification,” Proceedings of the 2008 International Conference on Information Warfare and Security (ICIW 2008), Peter Kiewit Institute, University of Nebraska Omaha, 24-25 April 2008.

[22] A. Bourdreau and G. Couillard, “System Integration and Knowledge Management,” Information Systems Management, Fall, 24-32, 1999.

[23] I. Spiegler, “Knowledge management: a new idea or a recycled concept?” Communications of the Association for Information Systems, 3, 20, 2000.

[24] T.D. Petrocelli, “Data Protection and Information Lifecycle Management,” Upper Saddle River, New Jersey, Pearson Education, Inc., 2005.

[25] C.J. Alberts, A. Dorofee, J. Stevens, and C. Wooky, “Introduction to the OCTAVE approach,” Pittsburgh, PA, Carnegie Mellon University, 2003.

[26] C. J. Alberts and A. J. Dorofee, “Mission Assurance Analysis Protocol (MAAP): Assessing Risk in Complex Environments,” Networked Systems Survivability Program, Carnegie Mellon University, 2005.

[27] J.F. Stevens, “Information Asset Profiling,” Pittsburgh, PA, Carnegie Mellon University, 2005.

[28] G. Gunnarsson and J.M. Steinarsson, “Approaching Information Valuation - For clinical research information,” Master’s thesis in Informatics, IT University of Goteborg, Gotteborgs University, Goteborg, Sweden, 2004.

[29] M.V. Van Alstyne, “A proposal for valuing information and instrumental goods,” Proceeding of the 20th International Conference on Information Systems Charlotte, North Carolina, United States Association for Information Systems, 1999.

[30] K. J. Soohoo, “How Much Is Enough? A Risk Management Approach to Computer Security,” Consortium for Research on Information Security and Policy (CRISP), Stanford University, 2000.

[31] C.T. Morrision and P.R. Cohen, “Noisy information value in utility-based decision making,” Proceedings of the 1st international workshop on Utility-based data mining Chicago, Illinois ACM Press, 2005.

[32] EO13292, “Executive Order 13292 - Further Amendment to Executive Order 12958,” as Amended, Classified National Security Information, 2003.

[33] T.H. Davenport and L. Prusack, “Working Knowledge: How Organizations Manage What They Know,” Boston, Harvard Business School Press, 1998.

[34] M.R. Endsley, “Toward a Theory of Situation Awareness in Dynamic Systems,” Human Factors Journal, 37(1), 32-64, March 1995.

[35] G. Taddaa, J. Salerno, D. Boulware, M. Hinman, and S. Gorton, “Realizing Situation Awareness in a Cyber Environment,” Proceedings of SPIE; Multisensor, Multisource Information Fusion: Architectures, Algorithms, and Applications, vol. 6242, 2006.

[36] W.P. Hughes, Jr. ed., “Military Modelig for Decision Making”, 3rd Edition, Military Operations Research Society, 1997.