Proceedings of the 2007 IEEE Symposium on Computational Intelligence in Security and Defense Applications (CISDA 2007)

Towards an Information Asset-Based Defensive Cyber Damage Assessment Process

Michael R. Grimaila, *Senior Member*, and Larry W. Fortson
Center for Information Security Education and Research
Air Force Institute of Technology
Wright-Patterson AFB, Ohio 45433-7765, USA
{Michael.Grimaila, Larry.Fortson}@afit.edu

***Abstract*—The use of computers and communication technologies to enhance Command and Control (C2) processes has yielded enormous benefits in military operations. Commanders are able to make higher quality decisions by accessing a greater number of information resources, obtaining more frequent updates from their information resources, and by correlation between, and across, multiple information resources to reduce uncertainty in the battlespace. However, these benefits do not come without a cost. The reliance on technology results in significant operational risk that is often overlooked and is frequently underestimated. In this research-in-progress paper, we discuss our initial findings in our efforts to improve the defensive cyber battle damage assessment process within US Air Force networks. We have found that the lack of a rigorous, well-documented, information asset-based risk management process results in significant uncertainty and delay when assessing the impact of an information incident.**

Keywords-command and control, situational awareness, information asset valuation, information dependency

I. INTRODUCTION

Information is a critical asset to modern organizations, but especially so for the military which uses information to conduct all aspects of operations [1]. Information is collected, processed, analyzed, distributed, and aggregated to support situational awareness, operations planning, intelligence, and command decision making [2]. Commanders often must make critical decisions based upon limited information. The quality, conciseness, and timeliness of the information used in the decision making process dramatically impacts the quality of their decisions. The need to incorporate technology to reduce response time and to increase decision quality is driven by the nature of modern fast-paced, high-intensity conflicts.

In 1995, Admiral William A. Owens recognized the expanding use and integration of technology in command and control systems, sensors, and weapons systems as a "system of systems" [3]. He identified that this trend would continue and result in increasing amounts of information that would need to be processed and aggregated into knowledge to provide commanders "Dominant Battlespace Knowledge." Subsequently, in his book "The Fog of War," Owens proposed a model for understanding the technology enhanced battlespace [4]. In his model, a commander would ideally have Dominant Battlespace Knowledge (the ability to see the whole battlespace in near-real time for situational awareness), Immediate/Complete Battle Assessment (the ability to have immediate feedback about his troops' actions), and Near-Perfect Mission Assignment (the ability to command his troops with as little latency as possible). Today, each of these elements is directly or indirectly supported by use of networked information systems which facilitate information processing, information dissemination, and operational process automation. This results in an environment where an information incident (e.g., a breach of confidentiality, integrity, and/or availability of an information asset) can result in mission degradation or failure [5].

Despite robust defensive measures, inevitably an organization will have to deal with an information incident. It is important to remember that an information incident can result from any number of sources including external attacks, insider attackers, natural disasters, human errors, infrastructure degradation, or equipment failure. When this happens, the organization's decision makers need an accurate and immediate assessment of how the incident impacts their organizational mission. In many cases, an information incident can have a domino effect whereby other information assets that are derived from the affected asset are also impacted. Therefore, it is essential to implement a formal, well documented, information asset-based risk management methodology that identifies and values critical information assets; quantifies mission dependence upon information assets; and assign control measures to protect information assets at a level commensurate with their value to the organizational mission. The implementation of such a methodology will provide the ability to quickly estimate the impact of an information incident and provide commanders with a cyber damage assessment in terms of their mission capability.

The remainder of this paper of this paper is structured as follows: In section II, we discuss the importance of accurate and timely damage assessment in military operations. In section III, we examine the existing defensive damage assessment process and identify shortcomings in information risk management. In section IV, we present a notional example that illustrates the need for improvement when conducting cyber damage assessments. Finally, in section V we present our conclusions and make recommendations for future work.

This work was supported by a research grant from the Air Force Research Laboratory (F4FBBA6227G001).

1-4244-0700-1/07/$20.00 ©2007 IEEE

II. The Importance of Damage Assessment

Accurate and timely damage assessment has been a critical determinate in the quality of command and control decision making since the dawn of organized warfare [6]. The need to quickly assess the impact of offensive operations against the enemy is critical because it enables the commander to efficiently plan future operations and to deploy assets in support of the stated mission objectives. Similarly, from a defensive perspective the commander must be fully aware of the current status of all of its support elements. The need for accurate and timely damage assessment is even greater in cyberspace where attacks can occur in milliseconds and may have a greater impact due to the complexity and interconnectedness of the information infrastructure. A failure to immediately detect, contain, remediate, and assess the damage following a cyber attack may result in other unforeseen higher order effects that may not be immediately apparent. Unfortunately, the application of traditional physical damage assessment methodologies to information resources often fails to produce meaningful defensive damage assessment following an information compromise [7].

The need for improved damage assessment in the cyber domain is not a new development. In 1995 the Rand Corporation conducted a series of exercises known as "The Day After" that were designed to simulate information warfare attacks and to measure the ability of organizations to respond to the attacks [7]. The results of the exercise identified numerous critical issues that must be addressed to improve the Department of Defense (DOD) response to cyber attacks. Among these was the need for "mandatory reporting of attacks to help better identify and communicate vulnerabilities and needed corrective actions" and "damage assessments to reestablish the integrity of the information system compromised by an attacker." Despite these critical findings, more than ten years later we still do not have a standardized operational damage assessment model to calculate and communicate the impact of information compromises within US Air Force (USAF) networks [8]. This fact is the primary motivation for our research.

A. Information Risk Management

Proper risk management of information assets is essential to building a foundation for an effective security program and making accurate cyber damage assessment [9]. Existing cyber asset risk management frameworks tend to have a technology-based focus instead of an information asset-based focus [10]. Unfortunately, focusing solely on technology often overlooks the actual value provided to the organization by the information assets [11]. An asset-focused framework enables identification of risks from an asset perspective; facilitates identification, valuation, and documentation of the assets; and lays the foundation for defensive cyber damage assessment [12]. We have found that the primary reason organizations tend to embrace technology focused risk management (if they conduct formal risk management at all) is that the technology resources are more tangible than information resources and therefore require a less subjective valuation assessment, and hence less "work." A majority of existing risk management frameworks are based on economic impacts because they are more tangible than other forms of impact metrics [13]. However, in a military operations context, economic metrics do not provide commanders with the information necessary to make quality informed decisions when their organization experiences an information incident. In many cases, what a commander first needs to know is the impact to their mission capability resulting from the information incident, not how much it will cost to remediate the incident.

B. Data versus Information

Data is the fundamental element that is processed, stored, and transmitted in cyberspace. However, data has no inherent value as it is solely dependent upon its external application to produce value [14]. Human utility organizes and aggregates data into usable groupings of contextual relationships that endow the data with "relevance and purpose" [15]. Through interpretation, data becomes information and is inherently associated with meaning [16]. Information, not data, should be the focus when enumerating and valuing information assets because it is contributes to the development of knowledge for use in all forms of decision making. Information is the core asset of cyberspace which drives the need for information asset focused security planning, risk management, and ultimately cyber damage assessment. The aggregation of information into explicit knowledge by a decision maker in conjunction with their tacit knowledge is the process by which informed decisions can be made. Figure 1 show a hierarchical representation of how the value increases as data is composed in information and then into knowledge to support decision making. In contrast, the tangibility of the value tends to be inversely proportional to the value. This is driven by the difficultly to quantify the value of the decisions unless provided a given static context. Standardized identification, definition, and documentation of information assets (and their value) is required when attempting to unravel the information interdependencies that often exist in large organizations [17]. Structured documentation provides the commander with visibility of where important information assets are located and the role that each information asset typically plays in support of the mission.

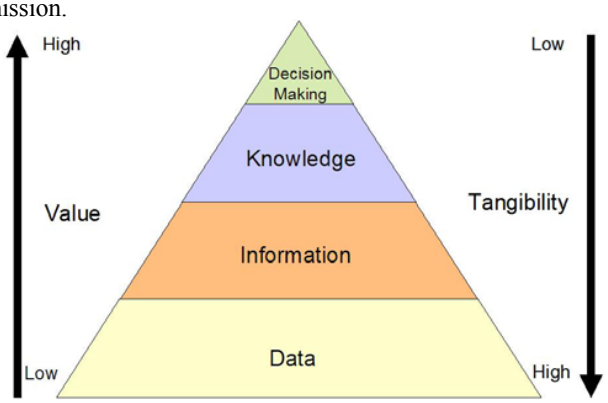

Figure 1. The Value Hierarchy

C. Information Production, Ownership, and Consumption

Information production, ownership, and consumption are easily and frequently confused due to the lack of standardized definitions. Information asset ownership is frequently assigned in organizations without regard to who created the information or where it originated. These issues are often irrelevant as long as the ownership of the information asset is established, the owner has responsibility and authority to perform ownership duties, and accountability is enforced [17]. In the complex domain of military cyber information flow, the roles and responsibilities of each group, by necessity, do not adhere to the traditional definition. This is especially true of the relationship between the information producer, information owner, and information consumer, where the clearly defined roles of consumption and ownership become relative to need. Information asset ownership gains a new fluidity, and becomes relative to the contextual value within an organization.

In a military context, an organization may receive intelligence information input from multiple external organizations, services, and countries. External information producers classify the information at the point of origin, but the classification only serves as a baseline valuation of the asset. As the organization stores and uses the information, the information also holds a contextual value depending on how the asset supports the organizational mission. At this point, the organization becomes more that just a consumer of the information asset; now the consumer is a "relative" owner. Relative ownership equates to static ownership for the purposes of risk management and damage assessment. Therefore, the information owner is responsible for identification, definition, valuation, and documentation of all information assets they "own." Each site where information asset ownership occurs, whether static or relative ownership, asset profiling must be accomplished by the information owner. The owner bears the burden since only the owner maintains a perspective that allows them to understand how the information is used to support the organization's mission, what the value of information asset is to the organization, and where the information asset is stored.

D. Information Asset Value Constructs

Determining the value of an information asset is a complex task, due to its inherent intangible qualities [18]. Many existing valuation models rely on economic metrics when conducting an information value appraisal. In the military, the intangible value of information often far exceeds its tangible economic value. The DOD possesses a distinct advantage in determining a baseline for the value of its information assets. All information stored on its networks is assigned classification through its uniform system for classifying, safeguarding, and declassifying national security information [19]. However, this only provides a coarse "first cut" for determining the value of information in the context of how it may impact national security.

Each organization that "uses" a given information asset in support of their mission will value that information asset based upon their own context or frame of reference. Contextual value is the most important component in information asset valuation. The constructs of the contextual value of information are mission binding, age, and state. Mission binding is a measurement of how closely the information asset is bound to the organization's mission through its supporting information process. An asset that is closely bound to an operational process will possess a relatively high value. If this asset supports an operational process that is critical to the organization's mission, the asset's value will be even higher. An understanding of how the value of information changes over its lifecycle must be accounted for when valuing information [14]. As information ages, its mission binding will often change. The failure to account for the temporal dimension of asset valuation often yields a valuation that seriously underestimates or overestimates the information assets value. State is the most fluid of an information asset's contextual value constructs. The state value is comprised of the information asset's level of confidentiality, integrity, and availability. An information incident can impact the state of the information asset causing resulting in an impact to all missions which are dependent upon it. A graphical representation of information asset valuation constructs is shown below in Figure 2.

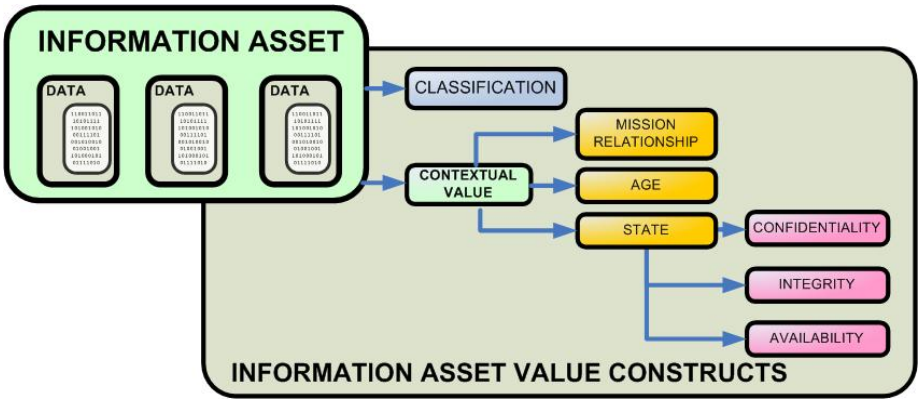

Figure 2. Information Asset Value Constructs

III. The Existing Defensive Cyber Damage Assessment Process in U.S. Air Force Networks

In this section, we discuss the existing defensive cyber damage assessment process in U.S. Air Force (USAF) networks. Note that we will focus on cyber damage assessment solely from a network defense perspective.

While there have been efforts within the Air Force to measure the impact to organizational mission following an information incident, the methodologies being employed are ad-hoc and without validation [8]. The metrics used to assess damage are economic, in terms of recovery costs and infrastructure availability. The Air Force Network Operations Center (AFNOC) Network Security Division (NSD) is the agency responsible for leading incident response efforts on USAF networks and regularly is requested to assess an the impact to an organization's mission capability following a successful compromise. This is an extremely difficult and often impossible task under the current implementation of security management practices on USAF networks. In this section, we briefly examine some of the factors that confound efforts to perform accurate and timely defensive cyber damage assessment, to include mission capability impact assessment, on USAF networks. Note that the problems identified in this discussion are not unique to the USAF or the DOD at large. It has been the author's experience that many of these problems are also present in public and private sector organizations.

A. An Infrastructure Approach to Network Defense

The USAF has implemented an infrastructure-focused network defense architecture. This traditional view of "cyber protection" is focused on the information systems and the infrastructure, rather than on the information assets contained within the information systems. This infrastructure-focused view acknowledges data existence, but substitutes the data's value with that of the infrastructure; and implies that by protecting the infrastructure, the data is protected. While this view has some merit, the assumption that technology is an equitable substitute for the information follows a proven path of failure [20]. The lack of documentation of critical information assets dramatically increases the time required to perform damage assessment. When an information incident occurs, commanders are unable to get an accurate or timely understanding of how their mission is impacted. One of the central reasons for this is that the traditional view relegates data as an incidental factor without appreciation for the value it provides as information to the organization's operations, and hence, its mission capability. As a result, critical information assets are not viewed in a way that requires their identification and documentation of the asset as would be done with a physical mission critical asset. When an information incident occurs, the Incident Response Team (IRT) is forced to conduct a mission impact assessment with little or no documentation that shows how what information assets are contained on the system, who owns the information assets, and the information supports the organizational mission. As a result, the damage assessment is based primarily upon economic factors (remediation and recovery costs) and availability. Subsequently, an effort is made to identify and quantify the impact by contacting a representative within the information owner's organization. Unfortunately, this often leads to a subjective and unreliable assessment of impact.

B. Lack of Effective "Cyber" Risk Management

Virtually all contemporary security planning methodologies include risk management as the foundation for a successful information security program [9]. The USAF understands the importance and benefits of risk management and employs risk management processes throughout the various aspects of its operations to achieve a high level of operations security. However, it fails to perform effective risk management of its information assets. The risk management that is accomplished is driven by the infrastructure focused mindset, resulting in documentation of technology rather than information assets. This is analogous to a risk management program documenting only the hangars on a flight line, but ignoring the aircraft within. If the hangar is destroyed, the commander will need to know how many flying and support assets were lost in order to assess their current mission capability. By simply documenting the container and infrastructure, the hangar facilities in this example, there is no way for the commander to rapidly and accurately know how the incident has affected his mission. Likewise, when a piece of cyber infrastructure such as a server experiences an information incident, only in rare occasions does the information owner understand which information assets were impacted. By failing to adequately implement enterprise risk management of its information assets, the USAF is finding itself blind, at both the unit and enterprise level, of the value of the information it depends upon to conduct its operations. As a result, bad command decisions may be made based upon an inaccurate perception of the cyber battlespace.

C. Lack of Information Asset Documentation

A lack of usable documentation of cyber information assets is a considerable problem that must be addressed in order to enable effective defensive cyber damage assessment. The USAF relies on its Operations Security (OPSEC) program to identify document critical information resources within an organization. Unfortunately, this program fails to adequately identify, valuate, and document cyber information resources in a manner that facilitates the accurate and timely understanding of mission impact following an information incident. In its current state of implementation, the USAF's OPSEC program is focused collecting information assets outside of the cyber domain. When digital information is documented, it is generally done so from a technical, rather than information, perspective. The OPSEC documentation is disjointed from the USAF's network security efforts and the

product it yields is unusable as a tool for assessing mission impact following an information security incident.

The traditional approach to cyber asset damage assessment attempts to determine the damage caused by an information security incident through assessment of technical impact to systems and/or infrastructure. Since data does not inherently possess value, this approach is fundamentally limited in its ability to measure impact in a value-focused manner. The ability to accurately measure mission impact following an information compromise is not possible using the current infrastructure-focused approach to damage assessment.

Figure 3 below depicts our understanding of how the existing incident response process works and how damage assessment is determined and communicated within USAF networks. When an incident occurs and is detected, the IRT is dispatched to investigate the incident as shown in step 1. The incident process conducted by the IRT will focus on investigation, remediation, restoration, and a preliminary damage assessment as shown in step 2. The IRT team will work with the system owners in an attempt to determine the impact of the incident. In many cases, the system owners are not fully aware of all of the information assets that are contained within the system. This is due, in part, to the dynamic nature of information systems and the fact that information assets are often deposited on (or deleted from) a system without the explicit knowledge of the system owners. Next, a preliminary assessment of the incident will be reporting through AFNOC NCD to all affected sites as shown in step 3. The reporting consists mainly of tangible technical metrics (loss of availability of data and the man-hours required to remediate the incident). Also, a subjective operational impact assessment will occur based upon how much knowledge the system owners have about the use of information stored on their systems. A mission impact assessment is virtually missing due to the lack of documentation of the information assets on the system and identification of organizations that depend upon the information. While it is true that the OPSEC program is tasked to identify and document critical information, OPSEC typically has a GWOT focus and is designed primarily to help reduce security breaches due to information leakage and correlation. Further, the OPSEC program as it exists today is not designed to provide a commander any mapping from information assets to operational or mission impact [8]. Segments of the security and defense world are attempting to address the problem, but there are formidable challenges to accomplishing the goal of accurate mission impact assessment. This is partially due to the continued focus on the 'tangible' infrastructure aspects and the failure to explicitly measure the impact to the information and information processes that actually make operations happen.

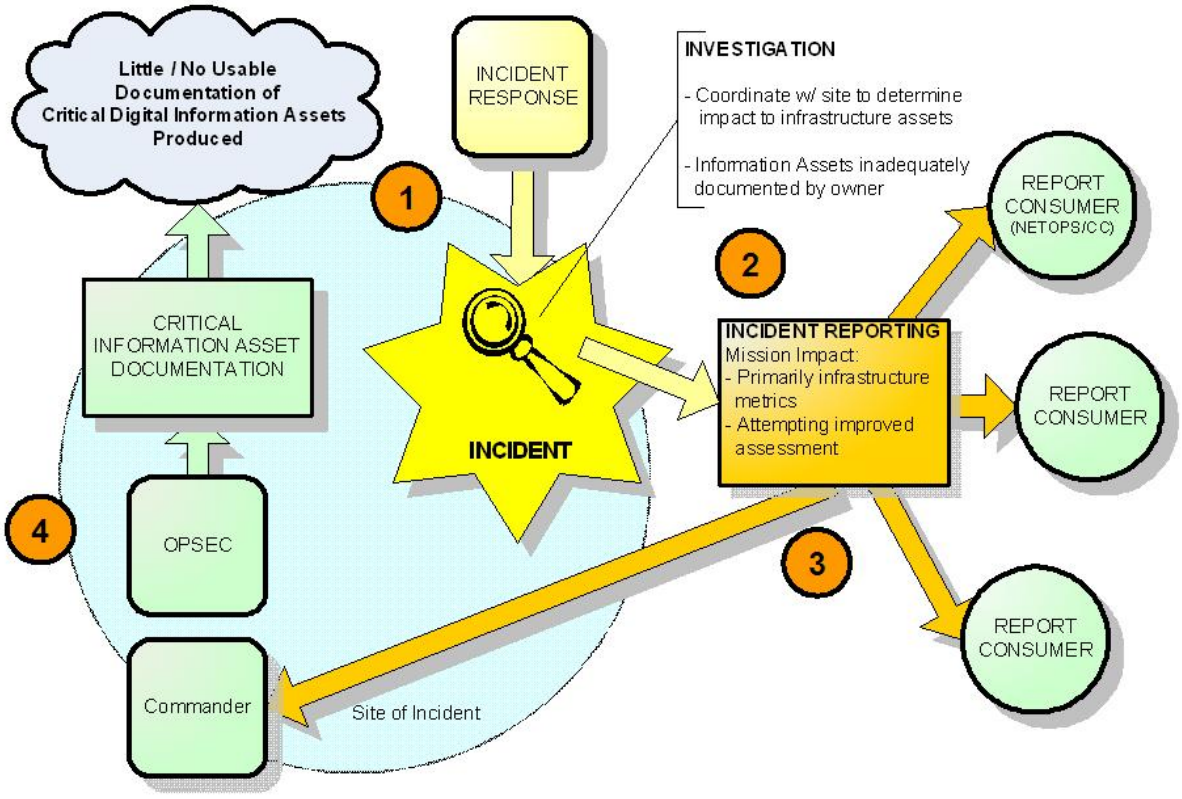

Figure 3. Current USAF Damage Assessment Process

IV. A Notional Example of Existing Defensive Cyber Damage Assessment

In this section, we present a notional example to illustrate the problems found in the existing cyber damage assessment process. While the example is fictitious, the problems discussed are real and can contribute to bad decision making with catastrophic consequences.

The purpose of defensive cyber damage assessment is to provide decision makers an understanding, in their context of operations, of the impact to mission capability following an information incident. Effective defensive cyber damage assessment depends on the identification and valuation of assets that are at risk; and what constructs of those assets are vulnerable to exploit. An incident may impact an information asset in such a way that it is less contributory (e.g. devaluation) to the organization's ability to accomplish its mission. If an incident impacts an asset so that it becomes unavailable or otherwise degraded, the operational processes that depend on it will also be degraded, in turn causing some degree of mission degradation. The degree of the mission impact will depend upon the role that the information asset plays in the command decision making process and the importance of the decision that is being made.

In the following examples, we consider how the impact from an information incident may be reported. For simplicity of this discussion, we assume that a compromise of an information system occurs that impacts the availability of a critical information asset. If the affected asset is a 'hot' asset, one that is being actively used in direct support of the organization's mission, the mission impact may be realized in a short amount of time. Since the asset is a critical mission asset, the organizational mission may be degraded or stopped in a relatively short amount of time. In this case, the mission impact will likely be readily apparent since critical mission systems may not be able to function effectively. Consider a analogous non-cyber scenario of a commander tasked to put bombs on targets X, Y, and Z. One half hour prior to the sorties departing, the enemy mounts a surprise attack on the base resulting in the destruction of 40% of the commander's mission air assets on the ground. The commander immediately understands that their mission capability has been significantly reduced. Likewise, if a live system is hit by an availability compromise, the effects are more obvious.

In some cases, mission capability may be affected by compromise of non-hot assets. A compromise may occur on a mission critical system that is not currently being used. If this system is critical to the organization's mission, but not used on a 24-hour basis and its ability to support the mission is degraded, for all practical purposes the organizational mission is degraded; just as if it had been a 'hot' asset. This is due to the fact that the system would not be available in the event mission requirements demanded use of the system. For example, consider a reserve flying unit that supports the in-theater commander. The unit depends on its classified systems to receive and process its sortie Air Tasking Orders. Now, suppose that a cyber incident results in this critical system being rendered unavailable for a few days. Since the unit was not actively flying, under existing damage assessment processes it would be reported that the incident caused no mission impact, which completely fails to account for the potential mission capability impact. For example, suppose that during the cyber incident, heavy air asset losses were suffered by the in-theater commander that required the unit's activation to support immediate in-theater operations. The reserve unit experienced mission degradation directly related to the incident resulting in an inability to rapidly mobilize its sorties in support of the theater commander. In this case the potential mission capability impact was not reported giving the theater commander an erroneous perception of his total mission capability. The theater commander is concerned with total mission capability. Therefore when we assess cyber damage to critical information resources, potential mission capability impact resulting from an incident must be reported with actual mission capability impact to determine the total impact to mission capability resulting from a cyber incident.

There are three key ideas that are illustrated by this example. First, a commander must know all of the critical information assets that it uses in prosecuting its missions. In order to accomplish this, there must be formal, documented recognition of information dependencies. Second, the commander must have real time situational awareness of all of the information assets that it "owns" that may be critical to executing it's mission. Third, when an information incident occurs it must be communicated to all downstream consumers of the information that may depend upon it in support of their mission capability. Thus, a commander needs the ability to know the status of external information resources that it may need to access, but may not be currently accessing in support of their mission. While this may be difficult under the existing risk management process, we believe that the combination of a well documented, formal risk management methodology in conjunction with automated tools could result in a process that could be implemented across the USAF.

V. Conclusions

In this paper, we have reviewed the existing USAF cyber damage assessment process, identified gaps in information risk management, and provided a notional example of the shortcomings of the existing defensive cyber damage assessment process. While the need for effective cyber damage assessment was recognized more than a decade ago, little progress has been made to attain this objective. However, the explosive growth of cyber attacks on military networks and the dependency on cyberspace to conduct military operations has awakened commanders to the shortcomings of current damage assessment capabilities.

We have identified that the USAF's distinction between information and information technology is obscured resulting in a negative impact on its approach to cyber security by placing the focus on information infrastructure rather than information assets. We stressed the importance of deliberate

security planning through an operations-oriented, asset-focused risk management process to lay the foundation for cyber damage assessment that maps to mission capability impact. An information asset focused risk assessment facilitates the identification of critical information assets within the infrastructure and results in the ability to documented and value information assets in a structured manner. This will enable the incident response function to work directly with the information owner to assess the mission impact resulting from the incident.

This paper represents the work we have completed to date to improve the quality and timeliness of defensive cyber damage assessment process. We continue to work towards developing a framework to operationalize the defensive cyber damage assessment process. We recognize that there are organizational dynamics, cultural issues, and resource constraints that need to be addressed and overcome to realize an efficient implementation of our perception of an ideal process. It is of paramount importance to automate as much of the information identification process to enable the practical application of the recommendations. We believe that our work will enable the development of a real-time situational awareness tool to provide commanders with a detailed understanding of cyber attacks in terms of their mission capability.

VI. 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] Joint Chiefs of Staff, "Joint Publication 3-13: Information Operations," United States Department of Defense, 13 February 2006.

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

[4] W. Owens, "Lifting the Fog of War," New York: Farrar, Straus and Giroux, 2000.

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

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

[7] 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.

[8] L. Theim, "A Study to Determine Damage Assessment Methods or Models on Air Force networks," Department of Engineering and Management, Air Force Institute of Technology, Wright Patterson Air Force Base, OH, 2005.

[9] 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.

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

[11] J. L. Spears, "The Effects of User Participation in Identifying Information Security Risk in Business Processes," Special Interest Group on Computer Personnel Research Annual Conference, Claremont, CA, ACM Press, 2006.

[12] 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.

[13] M. D. Horony, "Information System Incidents: The Development of a Damage Assessment Model. Air Force Institute of Technology, Wright Patterson Air Force Base, OH, 1999.

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

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

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

[17] J. F. Stevens, "Information Asset Profiling," Pittsburgh, PA, Carnegie Mellon University, 2005.

[18] 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.

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

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