Chapter

Challenges in Building Trusted Information Systems[1]

Serena Chan and Gregory N. Larsen
Institute for Defense Analyses
United States of America

1. Introduction

Globalization is a phenomenon that is bringing the world closer together through the exchange of raw goods, products, services, information, knowledge, and culture. Unprecedented advancements in technology, communications, science, transport, and industry have quickened the pace of global integration. The globalization process is creating and accelerating the emergence of transnational markets. Due to the presence of a worldwide market, there is a wider range of options to choose from among the products and services for building information systems.

The global supply chain and system complexity obscure "what's in the system." Systems are vulnerable to counterfeits, malicious inserts, or negligent design flaws. In today's global environment, one cannot afford to manage risks by simply seeking to avoid risks. The traditional discourse is that of risk avoidance. However, risk avoidance is untenable in an economic environment that operates globally with great variation in performance and with rapidly changing processes and technologies of consumption of production. Risks must be actively managed. Risk reduction comes at an expense with cost, schedule, and performance impacts to building trusted information systems. It may cost less to build robustness below some threshold of concern than to eliminate the risks, but it costs more than ignoring the risks. To find the right balance between the benefits, costs, and risks associated with globalization, one needs to understand how globalization works, the issues and challenges, and the subsequent system design and policy choices.

This book chapter discusses several research areas that address the effects of globalization coupled with the increasing complexity of building trusted information systems. The growing trend of globalization demands a more inclusive and persistent approach for actively managing risks in building trusted information systems. For example, the multifaceted, transitory, and global nature of the commercial information and communications technology (ICT) marketplace is limiting visibility into the supply and

---

[1] The publication of this book chapter does not indicate endorsement by the Department of Defense (DoD) or the Institute for Defense Analyses (IDA), nor should the contents be construed as reflecting the official position of those organizations.

suppliers. One of the main challenges is verification of trustworthy components and services in the design, development, test, production, deployment, operation, and maintenance of trusted information systems.

2. Globalization

Globalization is linking people and things at a faster pace than ever before. With global markets, supply chains have become more intricate, uncertain, and unpredictable. Therefore, globalization presents challenging problems to assuring the integrity of components used to build trustworthy information systems and networks. Critical information systems should be composed of parts that are trusted to do only that which is expected or specified and to do so reliably and dependably. Global supply chains are vulnerable to questions of unknown product or service provenance, which subsequently leads to questionable trustworthiness of the supplied items and the suppliers in the supply chain.

Both globalization and outsourcing are creating longer supply chains. Outsourcing creates a greater dependency on outsiders – procuring ever-more-complex and more critical products from external strategic suppliers instead of developing products in-house (Bolgar 2010). Outsourcing projects can provide a number of benefits, including cost savings, increased productivity, improved schedule performance, and higher quality of work (Kliem, 2004). However, extended supply chains greatly increase the complexity of the supply network and decrease the visibility of risks. Nevertheless, globalization provides an opportunity to increase the security of mission critical information systems. The global marketplace can be leveraged to propagate better information assurance techniques and security practices in designing and building trusted information systems.

3. Information Systems

An information system is specifically designed to operate on information, i.e., information is the flow variable in the system. In general, systems are designed for a purpose and have the following operational properties:

- Consume (ingest)
- Process (convert)
- Produce (output)
- Control signalling (regulate operations)
- Store (hold)

A system can be defined as a combination of hardware, software, infrastructure, and trained personnel operating to achieve specified mission objectives. This definition of system includes both the communications technology and information that is employed in addition to the way in which people interact with the technology.

Modern information systems increasingly rely on globally sourced ICT components and services. The variety and abundance in the marketplace is driven by the rapid decline in cost and the rapid increase in performance advancements. As supply is able to meet the

demand for low cost and more functions, today's information systems are increasingly complex in nature.

3.1 Trusted Information Systems

One foundation for building trusted information systems is systems assurance. Systems assurance is defined as the justified confidence that the system functions as intended and is free of exploitable vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system at any time during the life cycle (NDIA, 2008). The ideal scenario where no exploitable vulnerabilities exist is unrealistic. Therefore, active risk management must be performed to reduce the probability and impact of vulnerabilities to tolerable levels of risks.

Confidence establishes trustworthiness and tolerable residual risk. Trust in any information system is really the result of the methods employed to assure confidence in the system, both in its functions and protection of the information it holds and the results it produces.

4. Trust & Risk

Trust and risk are closely related. Trust can be described as the willingness to take risk (Mayer et al., 1995, as cited in Laeequddin et. al, 2008). Trust can be defined in terms of willingness to assume risk, intention in terms of willingness to assume risk, intention to make oneself vulnerable, acceptance of risk, and readiness to assume risk (Chopra & Wallce, 2003, as cited in Zuo & Hu, 2009). Meanwhile, risk is about choice; the action that is undertaken (Bernstein, 1996, as cited in Laeequddin et al, 2008).

Table 1 sorts risks into several basic categories and lists the areas they affect (Kleim, 2004). These risks are not necessarily mutually exclusive.

Risk Type	Affected Area
Financial	Budget and cost
Technical	Tools, techniques, and standards
Managerial	Decision making and reporting
Behavior	Managing and leading people
Legal	Governmental laws and regulatory considerations

Table 1. Types of Risks and Affected Areas

(Haimes, 2006) defines the following terms that have been broadly applied to risk analysis:

- *Vulnerability* – the manifestation of the inherent states of the system (e.g., physical, technical, organizational, cultural) that can be exploited to adversely affect (cause harm or damage to) that system.
- *Intent* – the desire or motivation to attack a target and cause adverse effects.
- *Capability* – the ability and capacity to attack a target and cause adverse effects.
- *Threat* – the intent and capability to adversely affect (cause harm or damage to) the system by adversely changing its states.
- *Risk* – the result of a threat with adverse effects to a vulnerable system.

The term 'susceptibility' is missing from the above list of definitions. The authors posit that one cannot manage risk unless there is an understanding of susceptibility. Understanding threat and vulnerability is necessary but not sufficient. Susceptibility is the intersection of threat (access) and vulnerability (opportunity). A viable threat requires access and a vulnerability provides an exploitable opportunity. A risk is realized when the susceptibility occurs at a certain instance or point in time. If threat and vulnerability intersect and there are no defenses, then the consequences of the realized risk must be tolerated (Chan & Larsen, 2010).

The nature of the risk being addressed in this chapter is fundamentally different from the current view of risk. The current view of risk focuses on vulnerabilities and motives to exploit the vulnerabilities. These risks are distinct from risks for which a threat actor makes deliberate investment to create an opportunity and trigger the realization of the risk for malicious purposes. Globalization creates conditions of supply that enable malicious threat actors to enrich their opportunities to craft susceptibility which may later be triggered to produce adverse consequences.

The class of risks that have gone unaddressed are those of supply chain exploitation, particularly exploits motivated by malice. These risks are the most difficult to detect. A malicious actor may not exploit vulnerabilities immediately but insert an opportunity to exploit at some point in the lifecycle development of the item of supply. The malicious actor's opportunity can occur at any time from cradle to grave. This type of malice is hard to detect because a threat actor has opportunity separate from the invocation of the risk to be realized. The malicious actor invests in providing "extra sauce" to the item of supply being consumed. Therefore, there is a need to counter invest to provide the ways and means that manage the risk of malicious exploitation of the supply chain.

Figure 1 illustrates susceptibility analyses as the center of gravity for risk management with respect to supply chain exploits. In a general context, any risk management effort needs a calculus that brings threats and vulnerabilities into coincidence to identify a risk of concern. Combining the identified risks of concern with an evaluation of how to reduce the adverse consequences of risk realizations enables the generation of a ranked list of susceptibilities. These susceptibilities provide input to risk managers to determine some combination of investments to reduce the impact of risks to mission tolerable levels of outcome that can be selected and implemented. This general approach is applicable to any specific class of all risks and contributes to the overall trade-space of risks to successful execution of mission performance.

4.1 Risk Management

Risk management is the process of responding to an event that offers negative or positive consequences. The goal is to maximize the gain from positive risks (opportunities) and minimize the loss from negative risks (Kliem, 2004). Risk management includes risk identification, risk analysis, and risk mitigation. Generally, the necessary steps to effective risk management are to (1) identify any potential risks, (2) assess the levels of threats, and (3) develop countermeasures and mitigations to reduce risks. Countermeasures are defined as actions or devices designed to negate or offset another whereas mitigations are defined as actions that can be taken to help reduce the impact of realized risks.

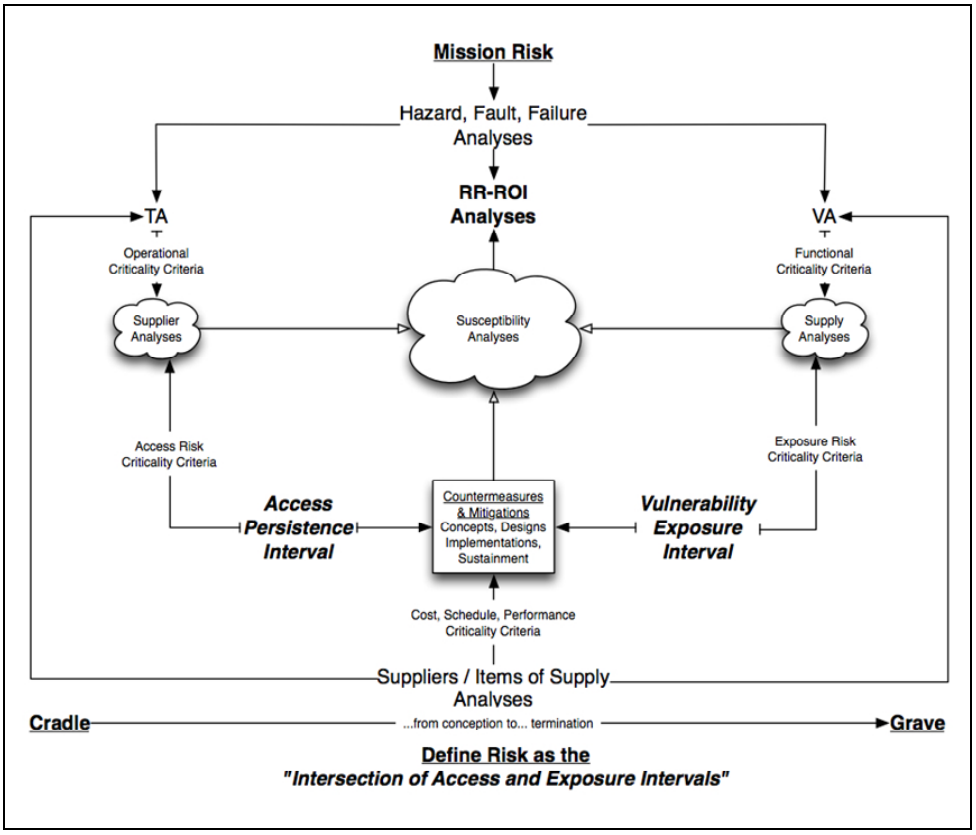

Fig. 1. Susceptibility Analyses as Center of Gravity

Qualitative analysis of the risk level helps to better prioritize risk (Khanmohammadi & Houmb, 2010) for obligating resources to reduce risk. After gaining a shared understanding of the impact and relative importance of risks, appropriate risk controls (Kleim, 2004) may be selected to be implemented:

- *Preventative controls* – techniques that mitigate the impact of a risk or stop it before having an impact (countermeasure).
- *Corrective controls* – techniques that involve determining the impact of a risk and require establishing measures to preclude future impacts (mitigation).
- *Detective controls* – techniques that reveal the existence of a risk and preclude future impact under similar conditions (vulnerability detection).

A traditional view in risk management is to "avoid risk." In reality, many people ignore risk because they do not understand it. However, risks cannot be ignored nor can all risks be eliminated. Attempting to eliminate all risks by applying countermeasures and mitigations is economically untenable. Residual risks will always remain. Due to these

factors, active risk management is required to establish tolerable levels of trust and risk. Furthermore, many existing risk management models are not applicable to supply chain networks. There is a lack of a satisfactory framework to analyze information risks unique to a supply chain network and to provide a structure to organize the deliberations and tools for managing supplier and supply chain risks for ICT components and services bound for trusted information systems and networks.

5. Research Areas

Globalization, more than many other factors, brings the uncertainties of an information operating environment into consideration of risks and the ways and means of countering and mitigating them. Furthermore, when the operating environment is a third party system of vulnerabilities, threats, intentions, capabilities, and risks for which every other system is dependent, the dynamics of the whole are considerably more difficult to assess, analyze, and apply actions to control or influence. The current research and development (R&D) agenda for single systems or systems-of-systems is more deliberate and explicit about particular characteristics of a system or collection of systems. While this work is improving the understanding of a "system," it is deficient in the totality of characteristics, knowledge, and techniques need to actually manage risks.

The authors suggest a paradigm of active risk management that requires a continuous feedback loop. Figure 2 illustrates a risk event timeline in three phases: pre-risk event, transitional risk event, and post-risk event. In each phase, there exist indicators and warnings to a potential risk occurrence. Vulnerability detection must occur at all times to seek out opportunities to prevent risks or mitigate risks to reduce impacts further downstream. Figure 3 illustrates the continuous feedback loop for active risk management. The activities for each of the three phases of active risk management seek to answer questions such as the ones listed below:

1. *Pre-Risk Event*: Identify and select risks to invest in doing something
    a) What can go wrong?
    b) What is the likelihood?
    c) What are the consequences?
    d) And at what time domain?
    e) What can be done and what options are available?
    f) What are the associated trade-offs in terms of all relevant costs, benefits, and risks?
2. *Transitional Risk Event*: Deploy countermeasures and mitigations
    a) What can be done and what options are available?
    b) What are the associated trade-offs in terms of all relevant costs, benefits, and risks?
    c) What are the impacts of current management decisions on future options?
3. *Post-Risk Event*: Evaluate the implemented countermeasures and mitigations, and readjust strategy if necessary
    a) What are the associated trade-offs in terms of all relevant costs, benefits, and risks?
    b) What are the impacts of current management decisions on future options?
    c) What can be done and what options are available?

Note that active risk management is a continuous cycle, with some of the same questions being asked and answered throughout. Further note that a risk must be experienced at least once, otherwise it just theory and not practice.

Fig. 2. Risk Event Timeline

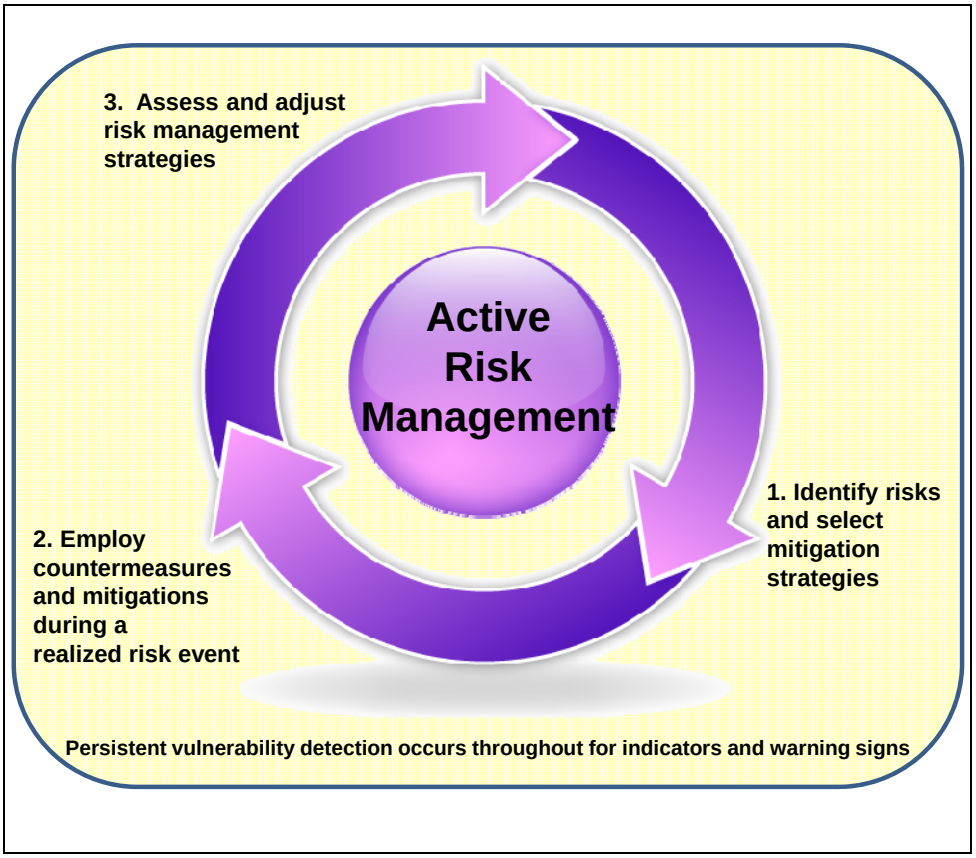

Fig. 3. Active Risk Management Activities

The effects of globalization set up a rich set of challenges, issues, and opportunities for research. Globalization further begs for a broad and interdisciplinary agenda of research to relate the pace, tempo, and interaction of the environment with information systems.

Current research is not driven by a totality of systems view nor does it deal with active management of risk. Modern and future dependence on information systems require a systematic development of research areas to deal with the problem space holistically. Otherwise, only partial knowledge and solutions are obtained because the focus is only on particular issues and solutions. A holistic perspective to identify risk and quality of implementation is therefore required.

5.1 Cyber Attacks

Cyberspace is a domain constructed by man and constantly under construction (Welch 2011). Modern information systems are connected to one another via networks. Functions essential to the computer control of the networks, information flowing or stored in the networks, and the decision support systems supported by the networks are subject to both physical damage and attacks that affect the logical realm. Table 2 maps six potential cyber attacks and their effects on information (Musman et al., 2011) and the impacted information assurance (IA) categories of confidentiality, integrity, and availability. Each 'X' represents an affirmative answer to the following question: Does the attack type, as defined, affect the IA category? Confidentiality refers to the prevention of unauthorized disclosure of data (both stored and communicated). Integrity refers to the prevention of unauthorized modification of data (both stored and communicated); detection and notification of unauthorized modification of data; and recording of all changes to data. Availability refers to the timely, reliable access to data and information services for authorized users. Availability attacks include destruction of assets and denial-of-service.

Table 2 highlights the importance of protecting integrity, yet this area is the least mature. Currently, there is a lot of research work that address confidentiality and availability. Most information systems assurance work deals with various malicious attacks that range from computer viruses, network penetration, and system breaches (Zuo & Hu, 2009). Availability can be preserved through asset diversity means (e.g., network path diversity). Confidentiality preservation mechanisms include authentication and authorization so that sensitive information is protected from unauthorized users. Encryption is a technique usually assumed to answer confidentiality and integrity issues. However, there is not much conducted research with regards to trusting the encryptor and protecting the integrity of information and data within an information system.

Figure 4 illustrates 36 potential situational-based mitigation categories that address integrity, confidentiality, and availability. Mitigations are time-dependent: pre-risk event, transitional risk event, and post-risk event. Potential risk management strategies can be classified as: prevention, remediation, mitigation, recovery, and reconstitution. Preventative strategies are usually derived from key and leading practices. Much research work is required to develop and organize the other types of risk management strategies. Figure 4 provides an illustrative framework to begin categorizing ways and means to manage risks represented by an action (applied pre-, trans-, or post-event) with an intended impact of the potential or actual loss of integrity, confidentiality, and availability.

		Information Assurance Categories		
Attack Category	**Effect on Information**	**Confidentiality**	**Integrity**	**Availability**
Degradation	Rate of information delivery is decreased; Quality or precision of information produced by an activity is decreased		X	X
Interruption	Information is unavailable for some time period			X
Modification	Information has been altered, meaning that the processes that use it may fail, or produce incorrect results		X	
Fabrication	False information has been entered into the system		X	
Interception	Information has been captured by the attacker	X	X	X
Unauthorized Use	Raises the potential for future effects on information	X	X	

Table 2. Information Assurance Impacts Due to Various Cyber Attacks

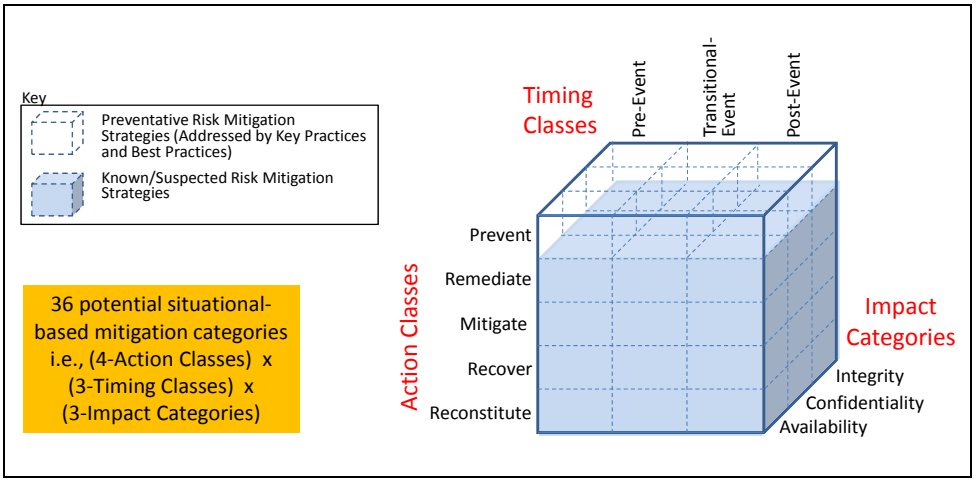

Fig. 4. Framework for Potential Risk Mitigation Strategies for Information Systems

5.2 Insider Threat

Most information security losses are due to the theft of proprietary information, a feat usually executed by insiders. An "insider" is stereotypically an employee, contractor, business partner, or anybody who has any level of legitimate access, driven by a wide range of reasons, both rational (e.g., money, status, power) and irrational (e.g., revenge, frustration, emotion pain, other personal problems) (Chuvakin, 2003). Insiders can be categorized by their intent into non-malicious and malicious insiders.

Non-malicious insiders compromise security due to their mistakes. Non-malicious users include people who want to "explore" the network or "improve" how things work without regard to security regulations. Non-malicious users present a hazard to the enterprise because they can incorrectly destroy information, degrade the availability and integrity of computing resources, and create opportunities for outsider attackers. Non-malicious insiders may also be unwitting participants, under the control of a malicious insider who uses social engineering techniques such as direct requests, persuasion, and other forms of deception. Hackers are known to evaluate the target information system, get initial information about the protective measures, and then launch social engineering attacks to enlist insiders to do their bidding (Chuvakin, 2003).

Malicious insiders are generally motivated by greed, a need for acknowledgment, sabotage, revenge, or a desire to be irreplaceable by creating problems only they can fix. Malicious insiders act to eavesdrop on a private communication, steal or damage data, use information in violation of company policy, or deny access to other authorized users (Chuvakin, 2003).

One proposed paradigm shift is to think of the supply chain problem as an insider threat problem. Because globalization expands insider access and knowledge of critical information systems to new populations, the information systems being built today are exposed to greater insider threat risk. The insider threat problem requires research in the areas of threat identification and appropriate countermeasures and mitigation. Moreover, the insider may not only be human. The machine (e.g., any logic-bearing or programmable ICT component) is a potential insider threat in an information system and network.

Most modern ICT are programmable and expected to execute operations with a degree of predictable variability. Unfortunately, this property of programmability enables malicious intent to also be implemented. This may take the form of design or incorrect implementation of design with residual vulnerability able to be exploited at one extreme. On the other extreme, it may be the deliberate insertion of programming intended to be exploited or triggered with the intent of malicious effect. The very property of programmability that gives great flexibility and range of utility is also an intrinsic vulnerability to be exploited from the outside (the most common form of threat exploit) or from the inside (the deliberate inclusion of programming that allows the device to behave as an insider – normal behavior in all respects until triggered to behave with intent to create malicious effects).

5.3 Vulnerability Detection

Detecting the human insider threat problem has been explored extensively. This concept depends on an understanding of correct behavior and the ability to observe the correctness

of expected behavior. Humans are "programmed" through cultural norms, training, and education to behave correctly. However, human-machine systems can be exploited by human insiders to exhibit anomalous behaviors.

Modern information systems have ICT-enabled advantages such as programmability. The programmability property provides variability that leads to flexibility which simultaneously gives rise to vulnerabilities. As the machinery of information systems has become increasingly programmable, complex, interconnected, and pervasive, the machine is becoming the means of malicious insider exploitation. Table 3 presents malicious vulnerability examples that can be inflicted by human or machine to another human or machine. Traditional methods of detection (e.g., behavioral approaches) are used to detect man-made vulnerabilities (e.g., conspiracies and hacking). Machine vulnerabilities may be inherent in the hardware equipment and requires human testing to detect. Globalization of the suppliers and the programmable nature of supplied items have vastly increased the opportunities for "insider behavior" implemented not by humans but by the machinery. The authors assert that an R&D agenda is required in counter-investment to understand, implement, and apply countermeasures and mitigations designed to meet what is functionally an insider threat realized in and executed by machine.

	Human	**Machine**
Human	Conspiracy	Hacking
Machine	Vulnerability	Operations Research

Table 3. Malicious Vulnerability Examples

As integrated circuit (IC) fabrication work is increasingly outsourced due to much lower costs, hardware manufacturers face significant security risks for ICs used in critical information systems and networks. Local, high-end, trusted facilities are economically unviable given the global economy. Further research work is required to address the uncertainty in provenance and hardware integrity. Example areas include digital IC fingerprinting and IC authentication tools and techniques.

5.4 Provenance & Supply Chain Visibility

Organizations are addressing new threats and opportunities presented by the question: "where does this stuff come from?" Due to the magnitude of the global sourcing issue and the multi-layered nature of the global supply chain, there are more variance and unpredictable factors in the environment to control. Therefore, a high level of supply chain visibility can be incorporated into the risk management processes to reduce product and performance related errors, and enhance the quality and responsiveness to risk incident occurrence (Tse & Tan, 2011). Due to the longer supply chains, it is critical to enhance the supply chain risk visibility by examining sub-tier suppliers and adjusting the supplier assessment process with the insights gained in a cyclic manner.

Issues of provenance can be applied to both physical artifacts and to information. Provenance can be identified in in two distinct ways: the source (or derivation) of an object and the record of the derivation (Moreau et al., 2008). Much of the provenance work has been applied to artifacts, especially in archives, art, and archaeology. Provenance has

recently become essential for digital documents in financial, commercial, medical, scientific, and legal contexts. Such information often originates in a remote location, gets processed by multiple parties, and resides in potentially untrustworthy storage (Hasan et al., 2009). In order to trust the information in a document, its provenance must be known because it is increasingly important to know where the information comes from and how it has been processed and handled.

More provenance research work is needed in the area of information and knowledge management, specifically electronic data. Electronic data does not usually contain historical information that would help end users, reviewers, or regulators. Process documentation is to electronic data as record of ownership is to a work of art (Moreau et al., 2008). A user's confidence in an application's electronic data can be increased by including the provenance that describes the process that led to the data's production. Digital data provenance tracking is useful for rights protection, regulatory compliance, management of intelligence and medical data, and authentication of information as it flows through information systems and networks. While significant research is being conducted in this area, the associated security and privacy issues have not been explored, leaving provenance information vulnerable to illicit alteration as it passes through untrusted environments (Hasan et al., 2009). Therefore, provenance of electronic data does not completely address or assure integrity.

5.5 Security & Privacy

Security and privacy have different requirements but share a point of intersection; security can be achieved without privacy, and privacy cannot be preserved without security. Security is provided by a "system" that handles information. Privacy begins with an accountable action taken by a user of information machinery. If the "system" consists of a user (human) and the machinery, then the information system can be designed to holistically intersect to provide security and privacy by employing machine handling of information to achieve both security and privacy protections. However, privacy begins with the human that enters information into the machine and authorizes its use and transmission by the machine component of the "system" or "network." No amount of machine security can guarantee privacy as privacy begins with the original provider of information into the machinery of the "system."

Security is about protection, whereas privacy is about permission and use of personally identifiable information (PII). Information technology systems can be built to the highest security standards without any regard to privacy. However, once PII is collected, security measures are necessary to preserve privacy (Federal Enterprise Architecture Program Management Office, 2006). A security policy may address information classification, protection, and periodic review to ensure compliance. However, privacy policies are needed to determine how security is implemented for the purposes of protecting PII within information systems. Elements of a privacy policy include information regarding the processes of information collection, analysis, maintenance, access, dissemination, and deletion.

Information security is defined as protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction (44 U.S.C. §

3542(b)(1)). As security is crucial for ensuring privacy, an initial look at how IA measures can deal with privacy concerns is provided. Table 4 provides a mapping of whether the IA categories can address the 17 privacy control families defined in *The Federal Enterprise Architecture Security and Privacy Profile* (June 2006). Each 'X' represents an affirmative answer to the following question: Can the standards and technologies of the IA category address and/or support the policies and procedures of the privacy control family. As Table 4 is a high-level view, each entry can be further examined in regards to specific standards, technologies, policies, and procedures.

	Information Assurance Categories		
Privacy Control Family	**Confidentiality**	**Integrity**	**Availability**
Policies and Procedures	X	X	
Privacy as Part of the Development Life Cycle	X	X	X
Assigned Roles, Responsibilities, and Accountability	X	X	
Monitoring and Measuring			
Education: Awareness and Role-based Training Programs	X	X	
Public Disclosure			
Notice			
Consent			
Minimum Necessary			
Acceptable Use	X		
Accuracy of Data		X	
Individual Rights			
Authorization			
Chain of Trust	X		
Risk Management			
Reporting and Response			
Security Measures	X	X	X

Table 4. Mapping of Whether IA Categories Can Address Privacy Control Families

The results of Table 4 draw out the following main findings:

1. The IA category of availability has a minimal relationship with privacy. Availability deals with system design to ensure high accessibility and redundancy of resources and capabilities.
2. While IA can address a majority of the privacy control families, IA does not address public disclosure, notice, consent, minimum necessary, individual rights, and authorization. Authorization in the privacy context refers to an individual's ability to authorize all new and secondary uses of PII not previously identified on the original collection notice. These privacy control families must therefore be addressed through another mechanism, such as business rules and processes.

3. The remaining privacy control families not addressed by the traditional IA categories are addressed by the expanded IA categories, which include assured information sharing, assured mission management, and system/network defense.

In summary, IA does not address every threat to protecting privacy and personal data. While IA relates to securing and protecting an information system, information privacy relates to an individual's right to determine how, when, and to what extent personal information will be released to another person or organization.

5.5.1 Insider Threat

With respect to privacy, there are two types of insider threats to consider: (1) insiders who have the correct permissions and authorizations for data access may deliberately misuse information and/or provide information to unauthorized parties and (2) insiders who may inadvertently misuse information due to ignorance or carelessness that may result in improper disclosure (Waterman, 2006). The second kind of insider threat as described poses the greatest danger to the appropriate protection of privacy data. While IA can provide measures to ensure proper authorization and access control, IA cannot tackle the use of information for purposes other than the one or ones for which it was originally collected. One way to consider addressing the insider threat issue is through policies and procedures that provide education and training on the appropriate use of information and through enforcement of these policies and procedures.

5.5.2 Data Mining Tools

Some data mining tools make automatic associations in such a way that even naïve users could deduce private information from the unclassified or public pieces of data by basically exploiting the associations made available by these tools. Thus, there is a need for the development of privacy-preserving techniques for PII data management (Ferrari & Thuraisingham, 2006). Data anonymization, masking, and filtering are methods being used to protect the rights of individuals and minimial disclosure. However, even these techniques can be subverted.

5.5.3 Appropriate Privacy Policies

Privacy policies are being used by organizations to tackle the issue of PII. However, few privacy policies actually assert that your PII will remain secret or private and under your control (Poore, 1999). In reality, a privacy policy is simply an information policy that tells you what information is collected and how it is used. It does not necessarily mean that your privacy is protected and may actually specify that privacy is not provided. The inability for individuals to agree in terms of what they believe is an appropriate privacy policy or practice is a major challenge to achieving consistent protection for groups of individuals. Privacy is not absolute. There are many trade-offs in the benefits versus the risks.

5.5.4 Transparency

The ability to balance the privacy concerns of individuals with effective monitoring of potential insiders is a very challenging task. One significant problem is that individuals often are not aware of the information that is collected and how it is used or what has been

done with it. In addition to the privacy conditions of notice, choice, use, and security, it is equally important to offer the privacy conditions of correction and enforcement. These six conditions associated with privacy are derived from the European Union's Privacy Directive and are briefly described in Table 5. Transparency protects not only the individual but the organization or company and promotes public trust.

Condition	Description
1. Notice	The individual has the right to know that the collection of PII will exist.
2. Choice	The individual has the right to choose not to have the data collected.
3. Use	The individual has the right to know how data will be used and to restrict its use.
4. Security	The individual has the right to know the extent to which the data will be protected.
5. Correction	The individual has the right to challenge the accuracy of the data and to provide corrected information.
6. Enforcement	The individual has the right to seek legal relief through appropriate channels to protect privacy rights.

Table 5. Mapping of Whether IA Categories Can Address Privacy Control Families

5.5.5 Privacy Implementation

Privacy breaches occur mainly due to the failure to develop the business processes around privacy. Privacy management should not be reactive. Protecting privacy and personal data should be an integral component in the development of information systems that involve PII. Privacy should be one of the most important priorities in the development of trusted information systems, not an afterthought.

Most importantly, privacy depends upon the human component of the system to handle and exchange information with the machine component in a manner that establishes accountabilities for it at the outset and at every opportunity during the use and exchange of tagged and marked information with privacy attributes. Most losses of privacy are the result of human mishandling of information or the failure of machinery to maintain security of the information as it is manipulated and handled according to privacy attributes that originate with humans. Frequently, human handling or the inability of machine components to preserve privacy attributes at exchange points are the primary reasons for privacy failures. Nonetheless, privacy failures are usually misattributed to security failures.

Privacy must be considered an integral part of the development and use of an information system. Privacy policies and procedures must be developed as part of the business process so that appropriate IA measures can be implemented to support them. Recall that security can be developed without privacy but privacy cannot be provided without security. However, security measures cannot address all privacy issues hence privacy must be considered from the beginning. Privacy management should not be an afterthought, reactive, or piecemeal.

The following recommendations are provided to help move forward in providing both security and privacy for information systems:

- Promote a more coordinated approach to security and privacy consistent with business objectives and the goals of efficiency and interoperability.
- Conduct a Privacy Impact Assessment (PIA) to determine the effects of information services and sharing initiatives on individual privacy. Elements of PIAs should include the following:
  - The information that is being collected,
  - Why the information is being collected,
  - Intended use of the information,
  - With whom the information will be shared,
  - What opportunities individuals will have to provide information or to consent to particular uses of the information,
  - How information will be secured, and
  - Whether a system of records is being created under the privacy policy.
- Develop a plan for evaluation and continued monitoring of the implementation of the privacy policy.

A significant gap in R&D is the interface between human and machine components of a system. Security is about the machine component. Privacy is about the human component and its interaction with the machine component.

In summary, an information system should have a privacy policy that publicly articulates that it will adhere to legal requirements and processes that enable gathering and sharing of information to occur in a manner that protects personal privacy interests. A well-developed and implemented privacy policy should also be transparent in order to protect the enterprise, the individual, and the public; and promotes trust. A well-developed privacy policy also ensures that appropriate IA measures can be taken to meet both security and privacy needs.

5.6 Supplier-Supply Chain Risk Management (S-SCRM)

Traditional research work in supply chain risk management involves activities and processes for planning, coordination, operation, control, and optimization of the supply chain. These efforts do not examine supply chain risks associated with the compromise or loss of product/service confidentiality or integrity. Supply chain exploits are the opportunities where adversaries can gain access, obtain knowledge, insert malicious code, or corrupt devices bound for information systems.

In recent years, supply chain risk management research work emphasizes the key role of managing the operational risks in multi-layered supply chains. The authors have presented an enterprise framework for characterizing supplier-supply chain risk management that captures the underlying complexity and scope of concerns to manage globalization of information and communications technology risks (Chan & Larsen, 2010). The holistic view provides a way to manage risk by bringing intelligence mitigations, technical mitigations, and business mitigations into a tradespace to reach a collective view and to review or adjudicate decisions to obtain a tolerable risk-reduction – return on investment in making

informed acquisition and procurement decisions of ICT components and services bound for trusted information systems and networks. Additionally, there have been a number of risk management decision models that may apply to managing supply chain quality risk, including supplier qualification screening, multi-sourcing, flexibility, and penalties levied for supplier non-performance (Tse & Tan, 2011).

Figure 5 illustrates a framework to assess strategy options for managing supply chain risks. Risks must meet a threshold of feasible realization to be considered for the application of countermeasures or mitigations. This figure proposes an approach to determine the feasibility of risk mitigation strategies by making a determination of susceptibility (previously defined as an intersection at a point or interval of time of a threat able to gain access with the exposure of a vulnerability). Note that this requires access and exposure to occur at the same point or during some interval of time in order to become susceptible to an adverse consequence. Thus, simply being accessible or being vulnerable is insufficient to gauge the degree of consequence. The coincidence of a threat and vulnerability may have quite different consequences depending on the time of coincidence and the particular mission operation underway. Consequences must be judged with respect to impact on mission and relative to the state of mission execution (a point or duration in time). An assessment can then be made on whether the system retains the risk and the associated impacts on mission performance or if the risk needs to be specifically countered or mitigated. Subsequently, an appropriate risk reduction strategy must be developed by both considering the existing counters and mitigations and the availability or potential for applying additional countermeasures and mitigations to diminish the impact. In some cases, the strategic outcome may require a change of operational concept, a redesign of the system or component in order to eliminate a susceptibility, alter the consequence impact, or develop more effective and affordable counters and mitigations, or in extreme cases abandon the system altogether.

In all cases, this collection of knowledge is applicable in an iterative manner to arrive at an approach that applies supplier and supply item countermeasures and mitigations at various points of risk realization – either in a general manner or very specific manner. This could be at the level of threat actor generally (avoid suppliers) or more specifically at the point of access to a vulnerability (know the supplier but assume the item of supply can become an insider threat). Similarly, one can deal with vulnerabilities. In the ideal case, exquisite knowledge and opportunity exist to deal with susceptibilities that give rise to intolerable risks. If not, then counters and mitigations can be developed and applied for an assumed or poorly understood susceptibility and the consequences implied to system performance if realized. In the end, no judgment can be satisfactory without some sense of the economic and mission impact of uncountered and unmitigated risks. At a minimum, the identification of susceptibilities and their potential consequences gives visibility to risk managers and the opportunity to understand the worth of engineering for securing of systems and the residual risks for which security is currently not possible or not affordable. These can then be used to rationalize and justify R&D to discover, invent, and innovate security measures, which if applied achieve dependable and economic implementations able to withstand this emerging insider threat of compromised machinery and its potential to behave as intended most of the time and to change behavior and become malicious at inopportune times.

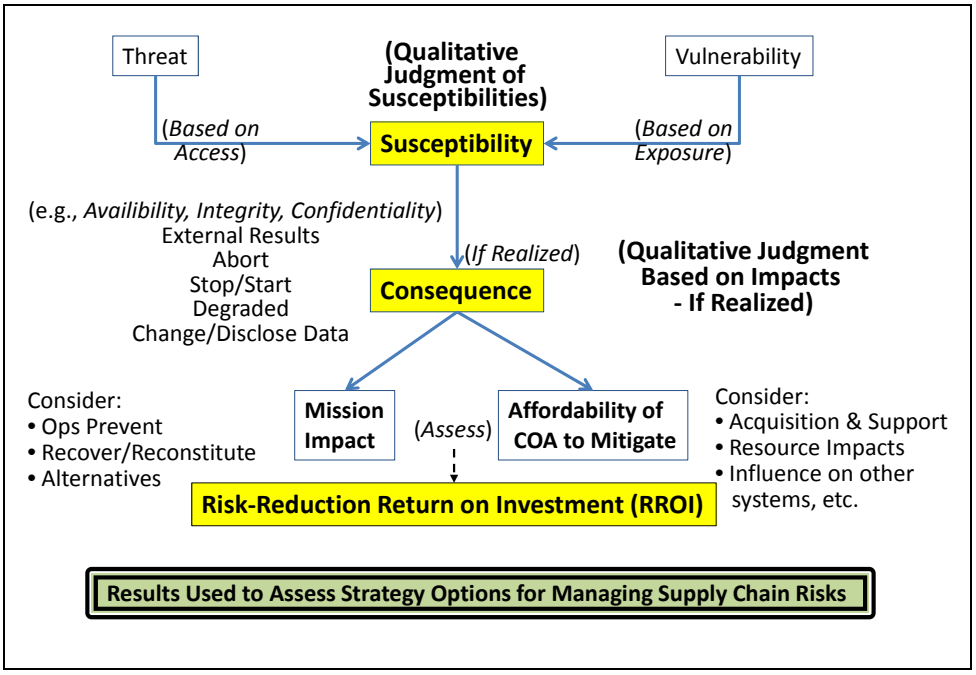

Fig. 5. Framework for Assessing Supply Chain Risk Management Strategies

The prospect that variable human-motivated and incentivized behaviors are the only insider behaviors to withstand by applying security measures is no longer wise given both the pervasive dependencies on ICT and the complexities and difficulties of having, maintaining, and sustaining provenance and visibility of supplied items and the production and delivery processes of their suppliers. The most basic need is to advance an agenda of R&D that recognizes today's security measures and countermeasures are not scalable to the new world order. This does not make the current research efforts unnecessary, but they are clearly not sufficient. The authors use the "label" of active risk management to capture the need for scalable means of identifying, implementing, and managing the application of countermeasures and mitigations for this growing set of risks that can never be fully prevented, eliminated, or avoided; but rather must be actively managed. Furthermore, the authors contend that the engineering for active risk management will stress the ability of traditional engineering disciplines, because it is likely to require risk management to be "built-in," not applied and forgotten. In the same manner that much rhetoric surrounds the "building-in" of security versus "strapping it on" like appliqué armour, active risk management will demand advances in design techniques, new and innovative ways and means of implementing countermeasures and mitigations, and vastly improved instrumentation to know the state of risk, the state of counters for such risks, and the invocation of countermeasures and mitigations on-demand.

5.7 Systems Security Engineering

Systems security engineering is defined in MIL-HDBK-1785 as "an element of system engineering that applies scientific and engineering principles to identify security vulnerabilities and minimize or contain risks associated with these vulnerabilities. It uses mathematical, physical, and related scientific disciplines, and the principles and methods of engineering design and analysis to specify, predict, and evaluate the vulnerability of the system to security threats."

Building more secure systems (i.e., security assurance in information technology systems) calls for the following requirements:

- Well-defined system-level security requirements,
- Well-designed component products,
- Sound systems security engineering practices,
- Competent systems security engineers,
- Appropriate metrics for product/system testing, evaluation, and assessment, and
- Comprehensive system security planning and lifecycle management.

Improving the security of information systems often relies on red teaming activities (Clem et. al, 2007) because they enhance knowledge in the following ways:

- Understanding adversaries and operational environments, assess threats;
- Anticipating program risk, identifying security assumptions, and supporting security decisions;
- Exploring and developing security options, policy, process, procedures, and impacts;
- Identifying and describing consequential program security;
- Identifying and describing consequential security design alternatives;
- Measuring security progress and establishing security baselines;
- Exploring security of future concepts of operation; and
- Identifying and describing surprise, unintended consequences.

Example red team activities (Clem et. al, 2007) and their objectives include the following:

- *Design assurance red teaming* – Helps ensure that a system will achieve its mission in degraded modes of operation.
- *Operational red teaming* – Helps to train staff, conduct testing and evaluation, validate concepts of operations, and identify vulnerabilities.
- *Penetration testing* – Helps to determine what access or control an insider, an outsider, or an outsider working with an insider may obtain.

The systems security engineering community needs to move toward designing for dependability, in addition to ensuring the other system "ilities" (e.g., affordability, availability, extensibility, flexibility, and scalability). Users of systems want the ability to trust that the systems (and services) will be consistently good in quality and performance. Trustworthy and reliable is the definition of dependable. Thus, securely engineering systems need to move in the direction of being dependable.

The authors posit that dependability is one of the missing specifications that enable a system security engineering community to be more effective through the lifecycle of a system development and to maintain effectiveness during operations and maintenance of a system. Without a specification of necessary and sufficient trustworthiness in the context of a system's use, it is extremely difficult to provide the arguments and demonstrations of the worth of security measures. They are often then subordinated in the engineering trade-space to other systems engineering factors (the other "ilities").

Dependability may serve as the property that combines security engineering with other engineering disciplines that lead to security being "built-in" versus "strapped-on." Security cannot be an afterthought. It must be built into cost, schedule, and performance. Not all risks are equal and not all users/consumers have equal tolerance for risks. Dependability establishes the value of security measures in a way that they legitimately become part of the engineering trade-space. It places a value on security measures that enable a value of worth during operations and use and serves as a metric for how well risks have been managed. Dependability may be the basis for integrating traditional "engineering of" systems (the partitioning with a defined system boundary and application of engineering disciplines) with the larger context of "engineering for" systems (the inclusion of the system environment that leads to the specification and definition of a system boundary).

5.8 Engineering Systems

"Engineering of" systems requires a holistic perspective that treats the operating environment of the engineering of a system concept, design, development, implementation, and support as more than an assumed and invariant actor that must merely be characterized and exploited by the system to be engineered. The operating environment "as a system" can be conceived, designed, developed, implemented, and supported to attain an advantage or benefit or present a risk. This is what distinguishes the "engineering of" versus the "engineering for" a system.

Systems engineering is defined an interdisciplinary approach to enable the realization of successful systems. It focuses on defining user needs and required functionality early in the development cycle, documenting requirements, and then continuing with the design synthesis and system validation while bearing in mind the whole problem: operations, cost and schedule, performance, training and support, test, manufacturing, and disposal. Systems engineering includes both the business and technical needs of all users with the objective of creating a quality product that meets the user needs. Systems engineering can fit within the overall engineering systems field. For example, systems engineering views the enterprise as a consideration or major influence on the system whereas engineering systems includes the enterprise as an essential part of the system.

Engineering systems is an emerging interdisciplinary academic and research field focused on addressing large-scale, complex engineering challenges with their social-political context. It takes an integrative holistic view of large-scale, complex, technologically-enabled systems with significant enterprise level interactions and socio-technical interfaces (Rhoades & Hastings, 2004). It may include components from several engineering disciplines, as well as

economics, public policy, and other sciences. It is suggested that the four underlying disciplines for engineering systems are:

- Systems architecture / systems engineering and product development
- Operations research and systems analysis
- Engineering management
- Technology and policy

Engineering trusted information systems requires active risk management. The definitions presented in Section 4 often lead to assessment and analysis results that fall short of what is required to fully manage risks; in particular, risks that originate in the operating environment (OE) of the system under analysis. Recent research has addressed a portion of this shortfall under the rubric of "systems-of-systems" considerations. However, much of this research simply alters the system boundary and applies systems knowledge and technique to a collection of interacting systems. Generally, this approach is distinguished by a deliberate and explicit focus on the interconnects among systems and how to influence or modulate each individual system to gain a better understanding of how the collective whole behaves as a "single system." Although valuable and important to the understanding of complex systems, emergent properties and behaviors of an interacting whole, and the relevance and significance of the linkages among systems as a system of its own, this approach does little to advance the study of managing risks.

Uncertainty is a fundamental source of risk. Managing uncertainty is the difficulty that hinders the successful management of risks. Uncertainty arises in the environment and propagates into a system or system-of-systems and back into the environment. These interconnections are shown in Figure 6. The carrier of uncertainty is information in information systems. This suggests that the information environment acts as an autonomous system, and is a third party actor for consideration in the management of risk. This third party originates uncertainties and has casual impact on both the structural interconnection among systems and the flow variables (information elements) that interact among the interconnected systems, and within the individual systems. The operating environment becomes a critical system when risk management is the objective. It may not be assumed away, avoided or ignored. This model of interacting systems of individual vulnerabilities, threats, intents, capabilities, and risks must be adequately characterized, modelled, analyzed, and evaluated as a whole. A risk event may originate anywhere, be propagated anywhere, be realized and have impact distant from its provenance, and be countered or mitigated anywhere. This is the dynamic that defines supply chain networks and the information risks they present.

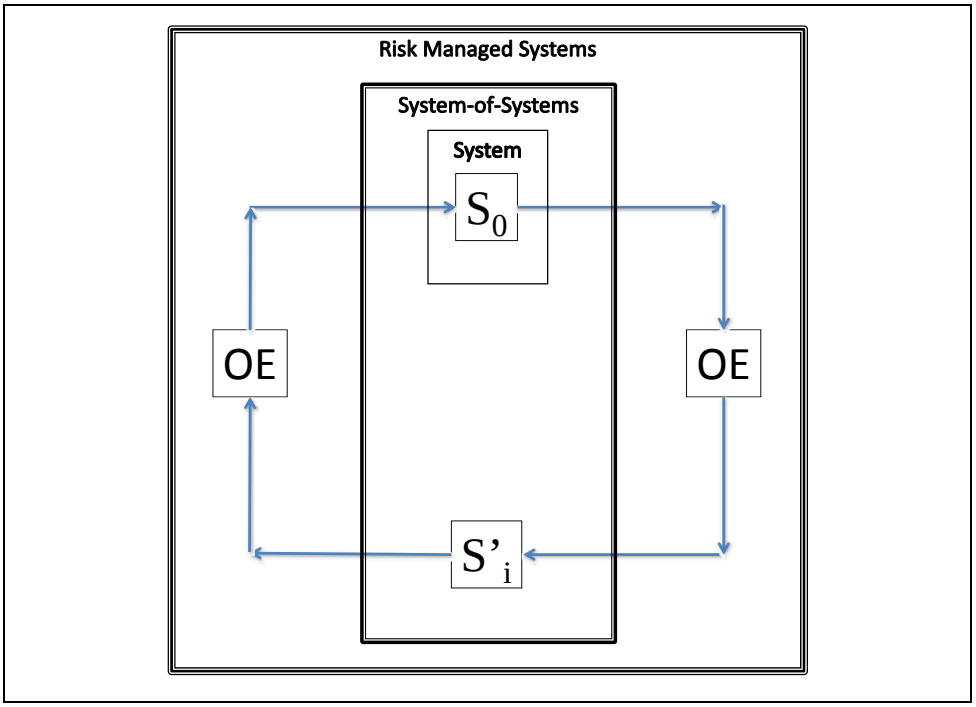

Fig. 6. Risk Managed Systems Framework

Modern dependency on ICT and the information operating environments creates challenges for today's system engineer in building trusted information systems. System complexity, coupled with the global sourcing of components and services, presents uncertainty in both the supplied items and the ways and means of producing the supplied items. The opportunities for "insider behavior" implemented not by humans but by the machinery of the human-machine system should alter the focus of R&D, the types and nature of countermeasures and mitigations implemented, and most certainly the tools and techniques of design, engineering, and test and evaluation, and operational monitoring.

6. Conclusion

A high level of confidence is needed in trusted information systems. There is a current void in active risk management research. Active risk management for building trusted information systems requires the following activities:

- Understanding mission tolerance to failures of integrity, confidentiality, and availability of information throughout the life-cycle of a product and the processes producing and maintaining it;
- Understanding system criticality and priority tolerance to risks to focus resources on appropriate and adequate countermeasures and mitigations;

- Understanding dependence on critical subcomponents and designing and instrumenting for robustness of risk management during mission operations and sustainment;
- Understanding supply chain for critical components and procuring within mission risk tolerance; and
- Partnering with industry to drive security (manufacturing, engineering, test and evaluation, etc.) into the processes and sub-suppliers at every production and support tier.
- Understanding that privacy is a trust threshold only enabled in part by mechanisms of security, the association of that trust threshold with a security capability, and the ability to maintain that security throughout the interactions among machinery components of the human-machine information system.

A research agenda in active risk management should include the following areas:

- Evolving the insider threat paradigm where the machine is the insider (both products and processes);
- Assuring information integrity and confidentiality throughout the life-cycle from idea to retirement from inventory;
- Improving supplier and supply item provenance and supply chain visibility;
- Enhancing testing and evaluation techniques for vulnerability detection of supply chain exploitation opportunities in the products and in the processes that produce and support them;
- Furthering systems security engineering to provide an understanding of the tools and techniques that discover and lead to effective and affordable countermeasures and mitigations.
- Developing the knowledge, inventing the technologies, and producing the innovations that recognize the differences between privacy and security while enabling the individual and organization to manage the risks of highly variable thresholds of trust and integrity of information employed and applied in human-machine information systems.

These areas of research are motivated by the effects of globalization and the tempo and pace of ICT advancement and application to complex information systems. The pervasive dependence and increasing strength of dependence requires correct systems behavior. An engineering systems approach to the problem and issues provides the holistic view to bring all the pieces together to understand the interactions and any emergent behavior of the information system as a whole.

7. References

Bolgar, C. (2010). Boosting Protection : Strategies for Reducing Risk and Staying Ahead of Your Competitor, In : *The Wall Street Journal Supply Chain Risk Insights*, 17.10.2011, Available from http://www.supplychainriskinsights.com/archive/scri-protection

Chan, S. & Larsen, G.N. (2010). A Framework for Supplier-Supply Chain Risk Management : Tradespace Factors to Achieve Risk Reduction – Return on Investment, *Proceedings*

of 2010 IEEE International Conference on Technologies for Homeland Security, ISBN 978-1-4244-6047-2, Waltham, MA, November 2010.

Chuvakin, A. (2003). Methods to Thwart Insider Attacks : Products, Techniques, and Policies, *Data Security Management*, Vol. 26, No. 1, (Feb/Mar 2003), pp. 1-11, ISSN 10967907.

Clem, J. F. ; Robbins, K. D. ; Parks, R. C. ; Mateski, M. E. & Page, K. J. (2007). *Red Teaming Quick Reference Sheet*. (25 April 2007).

Federal Enterprise Architecture Program Management Office (2006). The Federal Enterprise Architecture Security and Privacy Profile, Version 2.0, 1 June 2006.

Ferrari, E. & Thuraisingham, B. (2006). Guest Editorial: Special Issue on Privacy Preserving Data Management. *THE VLDB Journal*, Vol. 15, No, 4, (2006), pp. 291-292.

Haimes, Y.Y. (2006). On the Définition of Vulnerabilities in Measuring Risks to Infrastructures. *Risk Analysis*, Vol. 26, No. 2, (April 2006), pp. 293-296, ISSN 02724332.

Hasan, R. ; Sion, R. & Winslett, M. (2009). Preventing History Forgery with Secure Provenance. *ACM Transactions on Storage*, Vol. 5, No. 4, (December 2009), pp. 12-55, ISSN 1553-3077.

Khanmohammadi, K. & Houmb, S.H. (2010). Business Process-based Information Security Risk Assessment, *Proceedings of 2010 Fourth International Conference on Network and System Security*, pp. 199-206, ISBN 978-0-7695-4159-4, Melbourne, VIC, Australia.

Kliem, R. (2004). Managing the Risks of Offshoring IT Development Projects, *Information Systems Management*, Vol. 21, No. 3, (Summer 2004), pp. 22-27, ISSN 10580530.

Laeequddin, M. ; Sahay, B.S. & Sahay, V. (2008). Capturing the Concept of Trust Right in Supply Chain Partner's Relationship – A Conceptual Framework, In : *Journal of Knowledge Management Practice*, Vol. 11, Special Issue 1, (January 2010), Available from http://www.tlainc.com/articlsi11.htm.

Moreau, L. ; Groth, P. ; Miles, S. ; Vazquez-Salceda, J. ; Ibbotson, J. ; Jiang, S. ; Munroe, S. ; Rana, O. ; Schreiber, A. ; Tan, V. & Varga, L. (2008). The Provenance of Electronic Data. *Communications of the ACM*, Vol. 51, No. 4, (April 2008), pp. 52-58, ISSN 00010782.

Musman, S. ; Tanner, M. ; Temin, A. ; Elsaesser, E. & Loren, L. (2011). Computing the Impact of Cyber Attacks on Complex Missions, *Proceedings of 2011 IEEE International Systems Conference*, ISBN 978-1-4244-9493-4, Montreal, QC, Canada, April 2011.

National Defense Industrial Association (NDIA) System Assurance Committee. (2008). *Engineering for System Assurance*, (Version 1.0), October 2008, Available from http://www.acq.osd.mil/se/docs/SA-Guidebook-v1-Oct2008.pdf

Poore, R. S. (1999). Anonymity, Privacy and Trust. *Information Systems Security*, Vol. 8, No. 3, (Fall 1999), pp. 16-20, ISSN 1065898X.

Rhoades, D. & Hastings, D. (2004). The Case for Evolving Systems Engineering as a Field within Engineering Systems. *MIT Engineering Systems Symposium*, Cambridge, MA March 2004. Available from http://esd.mit.edu/symposium/pdfs/papers/rhodes.pdf

Tse, Y.K. & Tan, K.H. (2011). Managing Product Quality Risk in a Multi-Tier Global Supply Chain, *International Journal of Production Research*, Vol. 49, No. 1, (January 2011), pp. 139-158, ISSN 0020-7543.

Waterman, S. (2006). Analysis: DNI debates privacy rule changes, *UPI Security & Terrorism*, 21 August 2006, Available from http://www.upi.com/Business_News/Security-Industry/2006/08/21/Analysis-DNI-debates-privacy-rule-changes/UPI-47741156196154/

Welch, L. D. (2011). Cyberspace – The Fifth Operational Domain. *IDA Research Notes*. (Summer 2011), pp. 2-7.

Zuo, Y. & Hu, W. (2009). Trust-Based Information Risk Management in a Supply Chain Network, *International Journal of Information Systems and Supply Chain Management*, Vol. 2, No. 3, (July – September 2009), pp. 19-34, ISSN 1935-5726.

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188

1. REPORT DATE (DD-MM-YY)	2. REPORT TYPE	3. DATES COVERED (From – To)
November 2011	Study	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Challenges in Building Trusted Information Systems	DASW01-04-C-0003
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBERS

6. AUTHOR(S)	5d. PROJECT NUMBER
Serena Chan and Gregory N. Larsen	C5134
	5e. TASK NUMBER
	N/A
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES	8. PERFORMING ORGANIZATION REPORT NUMBER
Institute for Defense Analyses 4850 Mark Center Drive Alexandria, VA 22311-1882	IDA Nonstandard Document NS D-4495 Log no. 11-001788

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR'S / MONITOR'S ACRONYM
	11. SPONSOR'S / MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

This CRP product is an invited book chapter in the Open Access book, "Information System / Book 2," ISBN 979-953-307-585-2. This document was approved for public release: 15 December 2011.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Globalization is a phenomenon that is bringing the world closer together through the exchange of raw goods, products, services, information, knowledge, and culture. Unprecedented advancements in technology, communications, science, transport, and industry have quickened the pace of global integration. Due to the presence of a worldwide market, there is a wider range of options to choose from among the products and services for building information systems. To find the right balance between the benefits, costs, and risks associated with globalization, one needs to understand how globalization works, the issues and challenges, and the subsequent system design and policy choices. The growing trend of globalization demands a more inclusive and persistent approach for actively managing risks in building trusted information systems. This book chapter discusses several research areas that address the effects of globalization coupled with the increasing complexity of building trusted information systems.

15. SUBJECT TERMS

Globalization, Information Systems, Supply Chain Risk Management, Trust, Risk, Engineering Systems

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
Unclassified					Dr. Serena Chan
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER (Include Area Code)
Unclass	Unclass	Unclass	Unlimited	25	(703) 933-6563