Overview of Governance:

Help or Hindrance?

Author: Dennis P. German

Abstract

Human life on the planet has become ever more dependent upon the tools that are part of information technology systems (Carvalho & Mateus da Silva, 2003). And the task of keeping that human life safe and sound is no less the client of these systems. The US Department of Defense (DOD), its contractor as well as allies are effectively deaf, dumb and blind without information technology. Protecting the information processing capacity of these entities therefore rises to the highest priority. In this paper a notional paradigm is defined, gleaned from a variety of expert sources, which may well advance this effort. To that end each reference will be called upon to contribute insights into the policies and processes which entail the information assurance effort.

Straub, Goodman & Baskerville (2008) describe organizations struggling to define practical information security policies. A glance as the mind map reveals the cluttered factors to be considered; it is no wonder that an organization struggles with this process. The I&S Monitor (2006), a trade publication, provides dozens of sources to supplement the effort of security information systems. Though there are a myriad of courses, certifications and how-to plans there is no final or ultimate solution. But there is a reason for that; though from a high level all might seem alike, in reality no two systems are exactly the same. The context of an organization will be like a mold for the information assurance effort to be pressed into. As organizations have grown more dependent upon information systems they have also become more adept at managing security of their information systems. This has been seen in both the private public sector. Downtime as a result of a cyber-attack was shown to decrease from 26% in 2002 to 16% in 2003 while lengthy outages decreased from 39% to 26%. While this is partially attributed to improvements in the technology implemented for security purposes it can be seen that sound strategy has led to better management of information security practice (Straub, Goodman & Baskerville, 2008).

As the information technology industry has grown, so too has the community which support the implementation for an organization. This growth has been in large part due to the increasing complexity of an information system. This increasing complexity requires compartmentalized effort to maintain due to the level of knowledge required to perform each task. Management of this work must be focused on satisfying the needs of the user community so as to facilitate meeting customer requirements. A significant component of this work is within the information security discipline. This task is much more intricate than simply putting a lock on a door or a fence around an asset. The vectors of attack on an information system are at least in the tens of thousands. And this rough estimate only considers the virtual ports which exist within a computer's operating system. All of these angles of attack are available

to a malicious actor if the organization has a presence on The Internet. Therefore it is imperative that access to each organization be fortified by some means.

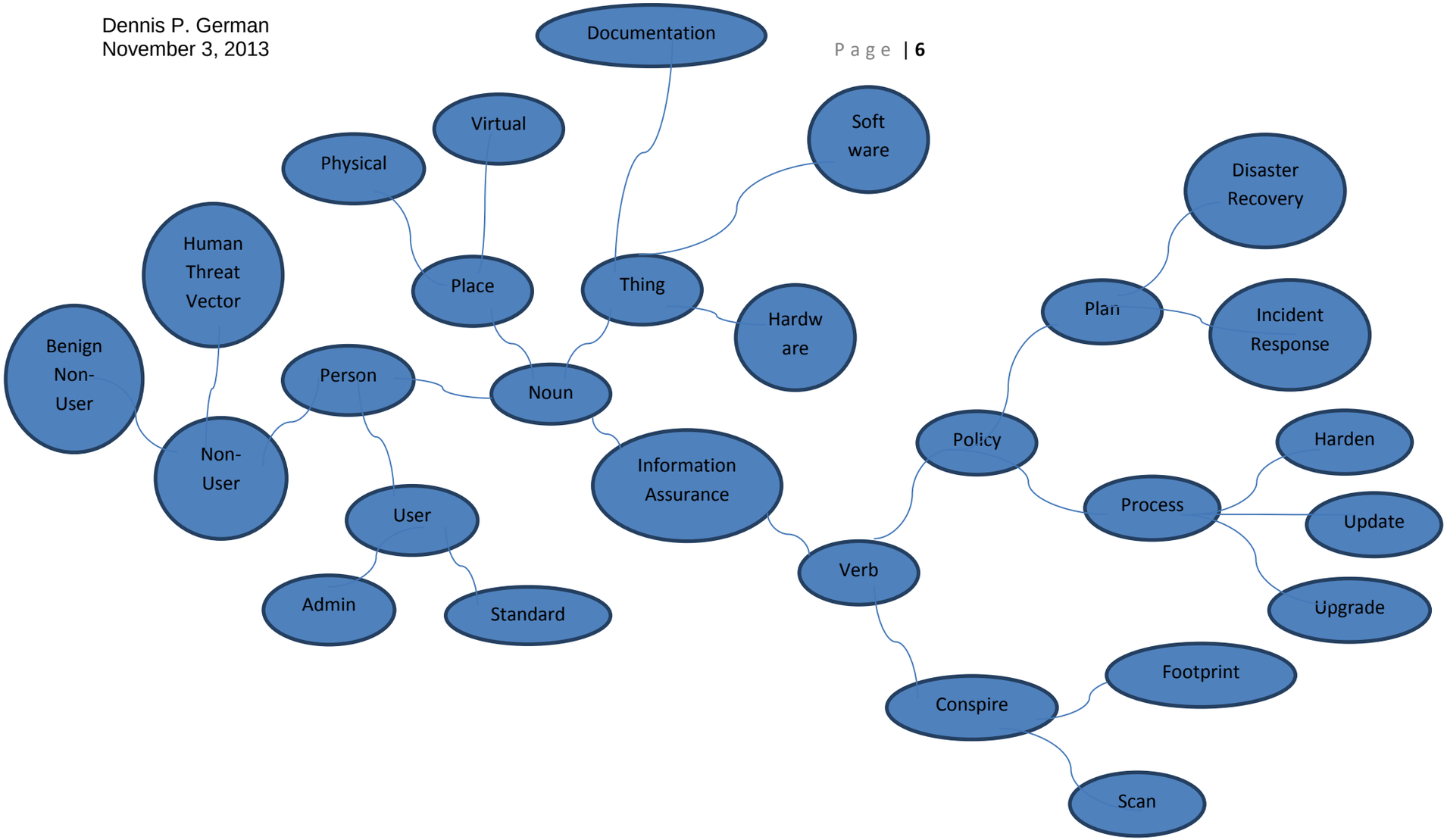
The science of securing an information system is called information assurance. This field of work deals with the definition of an information system from the policy documents (prior to it actually existing) to the disposition of the hardware at its end of life. The basic principles at work are confidentiality, integrity and availability. Ideally, the information assurance practitioner is engaged at the earliest possible time. This allows the system functional and operational specification to incorporate any required security facets. Information systems used by a company to process information for a DOD contract must meet the stringent requirements of the National Industrial Security Program Operating Manual (NISPOM). But as will any authoritative document applicable to an information system the NISPOM essentially brings to bear efforts (verbs) and tools (nouns) to combat the potential threats. Of course a tool set in many cases includes an individual to administer the software and hardware tools. Unfortunately, though a software or hardware tools might go awry, yet the personnel placed in the positions of responsibility to administer the tools can and do go awry as well. These personnel created negative impacts on an organization tend to be greater and farther reaching than those caused by an inanimate object such as a piece of hardware or software. The recent experience with the US Army and National Security Agency are perfect examples of this.

To partially deal with the human failure element there are various methods to estimate whether an individual is a security risk. Background investigations as well as psychological profiles and polygraph exams can unearth hidden behavioral issues that could present a possibility of compromise. The polygraph results (a favorite exam for the highest security clearances) are estimated to be 84%. Yet the prospect of having about one out of five subjects possibly getting through this who should not is a bit disconcerting (Jones, 2001). To further guard against insider threats an organization is expected to have

a separation of the differing functions as well as rotating assignments to preclude the possibility of collusion between users and administrators or any combination thereof. In the end, information system auditing and auditing of the auditors is an unending drill for information systems processing sensitive data.

It is improbable that one could positively determine the real efficacy of this effort. But it is assumed that this effort effective for the most part (Jones, 2001). Yet it does not require a large number of information system compromises to cause grave damage to US national security. In fact, only one breach is necessary to incur in inordinate amount of destruction. Thus it behooves us to employ efforts to reduce the possibility of introducing users, privileged and otherwise, who might be prone to unacceptable information system use.

The standards developed and implemented throughout the DOD contractor community to satisfy the NISPOM requirements generally are acceptable. Successful attacks on information systems are becoming few and far between (Winkler, 2007). It is only when there is some phenomenal compromise of data, such as the US Army and NSA having information ex-filtrated by insiders, that any such attack reaches the most common news media source. However, it would be advisable, for the DOD, to make adjustments to these requirements to provide controlling elements in a manner where the risk and effort/cost are compatible (Straub, Goodman & Baskerville, 2008).


Documentation
Virtual
Physical
Soft ware
Human Threat Vector
Place
Thing
Hardw are
Benign Non-User
Person
Noun
Non-User
Information Assurance
User
Admin
Standard
Verb
Policy
Plan
Disaster Recovery
Incident Response
Process
Harden
Update
Upgrade
Conspire
Footprint
Scan

References:

Naval Studies Board. Department of the Navy, (2010).*Information assurance for network-centric naval forces*. Washington, DC: Committee on Information Assurance for Network-Centric Naval Forces.

Carvalho, F., & Mateus da Silva, E. (2003, November). In Eduardo Mateus da Silva (Chair). Security in the information age. Presentation Nato advanced research workshop on cyberwar-netwar, Lisbon, Portugal.

Thomas, J., & Essaaidi, M. (2005, June). In Naoufal Raissouni (Chair). Information assurance and computer security. Proceedings of the NATO advanced research workshop on information assurance and computer security 2005, Tetuan, Morocco.

I&S Monitor. (2006). Cybersecurity related internet sources. Information & Security: An International Journal, 18, 137-147. Retrieved from http://procon.bg/node/1499

Straub, D., Goodman, S., & Baskerville, R. (2008). Information security: Policy, processes and practices. Armonk, NY: M.E. Sharpe.

Jones, A. (2001, November 2). *Summary of discussions at a planning meeting on cyber-security and the insider threat to classified information*. Retrieved from http://www.nap.edu/openbook.php?record_id=10197

Winkler, I. (2007). *Zen and the art of information security*. Rockland, MD: Syngress Publishing, Inc.

Under Secretary of Defense for Intelligence, (2006).*National industrial security program operating manual*. Washington, DC: U.S. Department of Defense.