

Creating an Internet Portal for INFOSEC Professionals

John W. Collins, Jr., Ed.D., *New Jersey City University*

Abstract – *This article briefly covers the need, feasibility and a potential solution for creating an Internet Portal for INFOSEC [1] professionals – in other words, access to an electronic knowledge base/dynamic. The major components are recommended to cover research, theory and sound practice within a multitude of INFOSEC environments: public, private, and non-profits. The connection to the major categories of the NSTISS 4011 standard is equally critical. The author proposes the establishment of an Internet Portal for INFOSEC professionals under the auspices of a neutral organization. One existing knowledge base portal was discussed to help skeptics see that this endeavor is very feasible. Additionally there are many connections for all members of a given learning community as well. This author is convinced that if the portal is built, many will come... so that our voices from within the professional security field can be heard, and more importantly shared.*

Index terms:

INFOSEC Education
Professional Security
Knowledge Base/Dynamic
Internet Portal
Theoretical Model
Learning Community

I. INTRODUCTION

All colleges and universities that have pursued the Information Assurance Courseware Evaluation (ICAE) Program for INFOSEC Professionals (NSTISSI [2] 4011) have personally experienced the scope and breadth of those standards. Some of us have mapped those components across a curriculum of five, ten or even more undergraduate or graduate courses. Our University approached the curriculum mapping requirement by modifying one existing course, adding two new courses, and now devotes all three courses entirely to the INFOSEC standards.

Dr. John W. Collins, Jr. is an Associate Professor and Graduate Coordinator with the College of Professional Studies, Department of Professional Security Studies at New Jersey City University in Jersey City, New Jersey. His contact information: Telephone – (201) 200-3179 and Email – jcollins2@njcu.edu

The current NSTISSI 4011 map for ICAE certification has a total of 256 elements within seven major categories. Yes, prior to being criticized too much by pure academics, we acknowledge there are some elements that are unique to the federal government level and our students may not encounter those facets in some work settings. As a Department, we decided our mission was best served by exposing all students to the entire spectrum of INFOSEC within NSTISSI 4011. At the major categories or top levels, we address: A. Communications Basics (awareness level), B. Automated Information System Basics (awareness level), C. Security Basics (awareness level), D. NSTISS Basics (awareness level), E. System Operating Environment (awareness level), F. NSTISS Planning and Management (performance level), and conclude with G. NSTISS Policies and Procedures (performance level).

II. A NEEDS ASSESSMENT

A quick environmental scan reveals there are several organizations involved in the INFOSEC profession. Some entities are governmental, others are private commercial and a few are non-profits. So the first question for problem identification: What are the needs in creating an Internet Portal for INFOSEC professionals? A traditional needs assessment may be too narrow or linear with the various intricacies of INFOSEC.

Most INFOSEC preparation programs are quickly evolving toward a scholar-practitioner approach by blending theory with research and proven practice. Perhaps such an evolution implies we are becoming learning communities – sharing our knowledge with protégés while creating a network of life-long learners. With the dynamics of professional security we need to be prepared to change as new threats and vulnerabilities emerge. Developing learning communities also must also be tempered with the understanding that our efforts may be undermined and infiltrated by those with less than pure hearts and motivation to learn about professional security and in this article, specifically INFOSEC. This is a unique balancing act to be sure.

Another aspect is the traditional academic concern of somehow disclosing intellectual property. In the field of

INFOSEC there are few truly individual ideas and concepts – and when they do occur, we quickly give attribution and citation. The reason INFOSEC knowledge and content works so well is that we have collectively used the information, policies, and procedures, time and again with acceptable results. Individual adoption may be possible, but the overriding knowledge base should be available for all INFOSEC professionals.

In reviewing some of the existing knowledge bases currently out on the Internet, we find a mixed bag. Some of the websites are trying to provide INFOSEC knowledge access and others using the location to recruit membership for their organizations. One or two are focused on certification.

This article does not specifically address all of the organizations already out there with their own approach to a portal or knowledge base. In fact, there are many. However, after a closer review most readers will find the portals and knowledge bases are organization-specific instead of being driven by the NSTISS standards (4011 in this article). For some examples, see the websites of ACM [3], INFOSEC@ NC State University [4], National Homeland Security Knowledge Base [5], NAVCOPS Knowledge Base [6], Responder Knowledge Base [7], Security Knowledge Base [8], and U.S. Security Awareness [9]. Certainly readers are aware of numerous other organizations. This very fact, that our potential resources are dispersed across the Internet affirms INFOSEC professionals have a need for consolidated information. INFOSEC resources shouldn't be thrown together helter skelter; rather we seek logical organization with a peer-review process that embraces accountability for content. The bottom-line as a profession: we need a synthesized and evaluated knowledge base.

III. THE MAGNITUDE

Today's INFOSEC professionals have to master a multitude of concepts, skills and competencies. This article is focused on NSTISS 4011 for content purposes, but this concept could be applied to all of the NSA IACE program standards: Senior Systems Managers, CNSSI [10] 4012; System Administrators (SA), CNSSI 4013; Information Systems Security Officers, CNSSI 4014 System Certifiers, NSTISSI 4015; Risk Analyst, CNSSI 4016; and any others under development.

Consider this partial list for instance from NSTISS 4011: agency-specific policies, AIS environments, AIS language, auditing and monitoring, capabilities and limitations of communications, COMSEC, concepts of trust, contingency planning, countermeasures, cryptosecurity, disaster recovery, facets of NSTISS, hardware, historical vs. current methodology, key management, legal elements media, life cycle management

management, legal elements media, life cycle management, memory, modes of operation, national policy and guidance, networks, network security, operations security, personal security, personnel roles, physical security, procedural controls, risk management, security planning, software, telecommunication systems, TEMPEST, threats, transmission security, vulnerabilities, and multitudes of forever-evolving changes or initiatives.

Although many of these topics have been associated exclusively with INFOSEC professionals for decades, other security professionals are becoming involved and nearly all of these subjects have succumbed to change. Change is certainly the expectation of most organizations — to the point it has become the only thing professional security leaders can absolutely anticipate. For a visual aid, review the list in Figure 1. The circle of arrows depicts the constant change. On top of this list, consider the various homogeneous and heterogeneous environments: private independents, public city, state, national, international, non-profit, not-for-profit, non-governmental organizations . . . and then add any of your own personal experiences. Tie this all together within the economic, political and social makeup of any particular organizational setting and we can *start* to understand the complexity of INFOSEC in the 21st Century.

agency-specific policies	memory
AIS environment	modes of operation
AIS language	national policy and guidance
auditing and monitoring	networks
capabilities and limitations of communications	network security
COMSEC	operations security
concepts of trust	personal security
contingency planning	personnel roles
countermeasures	physical security
cryptosecurity	procedural controls
disaster recovery	risk management
facets of NSTISS	security planning
hardware	software
historical vs. current methodology	telecommunication systems
key management	TEMPEST
legal elements media	transmission security
life cycle management	vulnerabilities and threats

Figure 1. Partial List of INFOSEC Concepts, Skills, and Competencies for Standard NSTISS 4011

IV. THE SILVER BULLET?

So why are some people convinced that a single concept can pull everything together like a magical silver bullet? The author is convinced that the typical critic has not been fully informed or educated. Even multiple silver bullets cannot fully encompass the majority of most organizational settings. Many non-profit organizations are constantly working to improve the knowledge base and access to the issues. A few examples include GIAC [11], (ICS)2 [12], ISACA [13], IT-ISAC [14], and SANS [15].

This article is designed to be a primer for evaluating, analyzing and synthesizing all of the resources that are currently available, using technology, specifically the Internet. Not wanting to be categorized as a techno-zealot, the author leans on the thesis of Neil Postman [16]. Postman advocated our careful and deliberate thinking with the use of technology; even to the point that our societal fabric can become unraveled when interpersonal relationships are overlooked due to the inherent anonymity aspect of technology.

V. AN INTERNET PORTAL

Consider the possibility of pulling everything together into a location or space: an Internet portal for INFOSEC professionals. Granted, the size of the information and data makes this a rather large space—more like a warehouse, but still accessible from a single and unbiased location. The Library of Congress (LOC) is a great example for books, periodicals, etc. We need our own LOC for INFOSEC professionals. This is especially critical in view of potential biases and slants of information for commercial and not-for-profit chartered organizations. The current term is a *portal* to multiple data sources and information that can be accessed using the Internet. This concept works by having a central gateway to the information: research, theory, informed practice, and any list can be built upon. It is actually three-dimensional, with connections to height, width and depth of a particular INFOSEC topic.

The entire idea sounds like another ivory-tower approach that an academic dreamed up during a professional conference. With the foregoing backdrop, how is this approach different? First, the responsibilities of INFOSEC professionals are real—not ivory-tower metaphors. Information needs to be readily available and accurate to deal with daily and often critical professional security issues. There must be an ability to tailor the information request to the various environments. For instance, what may work in a private corporation is not necessarily generalizable to a federal government setting and vice versa. Second, if we carefully select reliable information sources and group by themes we accomplish dichotomous sharing: one axis that provides information

in different INFOSEC environments (research, theory, practice) and another axis that ensures we consider the various NSTISS categories. (See Figure 2) Try to imagine the LOC and a warehouse. Both are huge entities. Without thoughtful organization, quickly finding a specific item is next to impossible. The proverb “like trying to finding a needle in a haystack” seems to be a perfect fit for our situation.

INFOSEC professionals are not dealing with a single dimension in the field. There are situations that require access to research, theory and proven best practices. Without having a synthesized portal, an already complex profession becomes even more onerous.

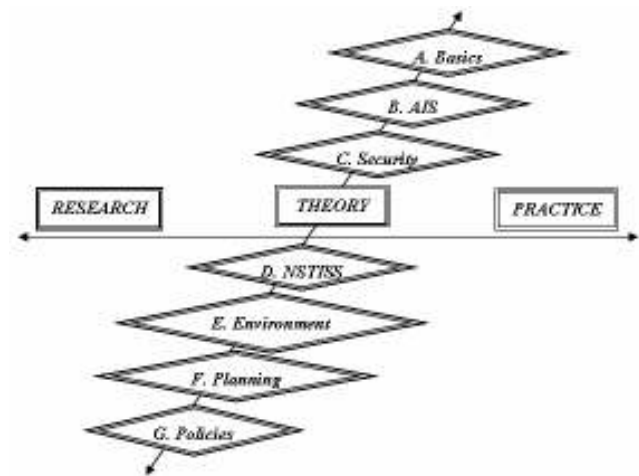


Figure 2. Axes of the NSTISS 4011 Standard - Knowledge Base/Dynamics

VI. FEASIBILITY AND CHALLENGES

After additional reflection readers may still be skeptical. This is too much pie-in-the-sky for many. Postman would remind us to clearly think through any potential uses of technology with the human dimension clearly considered. So it is imperative that INFOSEC professionals can communicate and network with each other. GREAT, yet another requirement added to the concept. How is this all possible? The author recommends using a portal model that already works. The military has at least one (actually there are several). It belongs to the United States Army under the name of the Army Knowledge Online (AKO). The author has access to this portal due to his retirement from that service after nearly 23 years of active duty. The portal can be personally adjusted with a specialized profile. In other words the opening screens can be

modified to deal with all the issues addressed in this article.

There is also the capability to network and email colleagues from within the portal. Sections of the user profile could cover corporations, independents, non-profits, and not-for-profit organizations. As a conceptual framework, view Figure 3.

This framework is just a starting point, not some all-inclusive model carved into stone. Additions and modifications are expected and needed for all learning communities. The dialogue needs your input. No matter how careful a particular organization is at assembling information, the preponderance is constituent-based. More succinctly stated, organizations are products of our social, economic and political systems. The author proposes the establishment of a INFOSEC portal that puts many silver bullets into a single warehouse—a warehouse full of silver bullets or at least entry points to the required information.

Further, this effort should be sponsored by a neutral organization that is motivated solely by the prospect of improving the INFOSEC profession. No one individual or groups of individuals can build this portal. It will take the collaborative efforts of many INFOSEC constituencies. The point here is that all INFOSEC knowledge and information needs to be available through one portal. There should be no commercials, advertisement or marketing: truly a neutral organization. Additionally, there are many connections in this portal for supporting all members of a given learning community, e.g. educators, current entry-level practitioners, mid-level security managers, professional security executives, etc.

A Potential Internet Portal for INFOSEC Professionals



Figure 3. A Conceptual Framework—Potential Categories, Topics, Hyperlinks, Resources, etc. (What, How and Why for INFOSEC Professionals).

VII. CONCLUSION

This article briefly covers the need, feasibility and a potential solution for creating an Internet Portal for

- ¹ INFOSEC – Information Systems Security. (2007). *Information assurance courseware evaluation (IACE) program*. Downloaded/address confirmed on March 1, 2007: <http://www.nsa.gov/ia/academia/acad00001.cfm>
- ² NSTISSI – National Training Standard for Information Systems Security. (2007). *National information assurance education and training program*. Downloaded/address confirmed on March 1, 2007: <http://www.nsa.gov/ia/academia/cnsstesstandards.cfm>
- ³ ACM – Association for Computing Machinery. (2007). *Association for Computing Machinery, the world's first educational and scientific computing society*. Downloaded/address confirmed on March 1, 2007: <http://www.acm.org/>
- ⁴ INFOSEC@NC State. (2007). *INFOSEC @ NC State University*. Downloaded/address confirmed on March 1, 2007: <http://ecommerce.ncsu.edu/infosec/>
- ⁵ National Homeland Security Knowledgebase. (2007). *Resources - homeland security resources, homeland security advisory system, HSAS, federal organizations and resources, homeland security directories, homeland security newsletter, homeland security sectors, homeland*

security products, homeland security companies, homeland defense, homeland security research, homeland security information resources, homeland security marketplace, homeland security RSS news feeds, homeland security blogs. Downloaded/address confirmed on March 1, 2007:

<http://www.twotigersonline.com/resources.html>

- ⁶ NAVCOPS Network – Naval Law Enforcement Network. (2007). *NAVCOPS Network|Knowledge Base*. Downloaded/address confirmed on March 1, 2007:
<http://www.navcops.com/information/categories/INFOSEC+%7B47%7D+OPSEC/>

- ⁷ Responder Knowledge Base. (2007). *Responder Knowledge Base - Please Log In*. Downloaded/address confirmed on March 1, 2007: <https://www.rkb.mipt.org/>

- ⁸ Security Knowledge Base. (2007). *ITtoolbox Security Knowledge Base*. Downloaded/address confirmed on March 1, 2007:
<http://security.ittoolbox.com/>

- ⁹ US Security Awareness. (2007). *Information Security Professional*. Downloaded/address confirmed on March 1, 2007:
<http://www.ussecurityawareness.org/highres/infosec-prof.html>

- ¹⁰ CNSSI – Committee on National Security Systems Instruction. *Instructions*. Downloaded/address confirmed on March 1, 2007:
<http://www.cnss.gov/instructions.html>

- ¹¹ GIAC – Global Information Assurance Certification. (2007). *Information security certification from GIAC*. Downloaded/address confirmed on March 1, 2007: <http://www.giac.org/>

- ¹² (ICS)2 – International Information Systems Security Certification Consortium. (2007). *(ISC)²*. Downloaded/address confirmed on March 1, 2007: <https://www.isc2.org/>

- ¹³ ISACA – Information Systems Audit and Control Association. (2007). *ISACA – Serving IT governance professionals*. Downloaded/address confirmed on March 1, 2007:
<http://www.isaca.org/>

- ¹⁴ IT-ISAC – Information Technology-Information Sharing and Analysis Center. (2007). *IT-ISAC*. Downloaded/address confirmed on March 1, 2007: <https://www.it-isac.org/>

- ¹⁵ SANS – SysAdmin, Audit, Network, Security. (2007). *SANS institute - network and computer security training*. Downloaded/address confirmed on March 1, 2007: <http://www.sans.org/>

- ¹⁶ Postman, N. (1993). *Technopoly: The surrender of technology to culture*. New York: Vintage Books.