An Introduction to the DHS EBK: Competency and Functional Framework for IT Security Workforce Development

Wm. Arthur Conklin

University of Houston, College of Technology
312 Technology Bldg, Houston, TX 77204
waconklin@uh.edu

ABSTRACT

One of the foundational elements of an information security program is an effective training and awareness program associated with the topic. A major challenge exists in determining who needs what level of information security training in an organization. The Department of Homeland Security was charged with determining the proper level of cybersecurity training and awareness across the federal sector for all non-classified systems. In response to this challenge, DHS has developed and released a document detailing a general framework to manage this critical HR function. This paper examines the usefulness of this framework and how it can be applied across organizations to address this critical element of an information security program.

INTRODUCTION

The Department of Homeland Security, National Cyber Security Division, has developed an Essential Body of Knowledge (EBK) for Information Technology (IT) Security (DHS 2008). Billed as a "Competency and Functional Framework for IT Security Workforce Development", the key feature is its ability to act as a framework for getting a handle on the complex nature of security workforce development and institutional security needs. Cyber security is a rapidly changing venue driven by changes in technology, changes in society as they adopt technological solutions and an ever increasing economic dependence on computer based transactions. As institutions and corporations expand their digital presence via the Internet, and as the digital generation enters young adulthood, society is being transformed by this digital communication based revolution. And as society changes, so does the criminal element, adapting to the new methods of trade to illegally obtain a piece of the action (Allenby and Fink 2005).

Defending against the criminal element requires a three pronged attack. Developers of the digital world need to design security into their products, reducing the risk of undesired actions. System operators need to understand the security ramifications of their systems so that they can manage and operate them both efficiently and securely. Finally, law enforcement needs to have the skills to recognize, investigate and prosecute criminal activity in this new digital realm. All of these issues relate to proper training of personnel. Add in the dimension of the continually evolving nature of digital society and you have an ever evolving set of training requirements. These training requirements differ based on both roles and environment across the security workforce (Theoharidou, Stougiannou et al. 2007; Shaw, Chen et al. 2008). The EBK attempts to capture the nature of this problem in an easy to use framework, and does so with remarkable clarity and flexibility.

This paper will examine the basics of the EBK and will demonstrate how the EBK framework can be crafted to a specific model to fit the needs of any particular institution. By demonstrating how to transition from framework to functional model, the power and generalizability of the framework will illustrated. The paper is organized as follows, a brief description of the component elements of the EBK followed by examples of how the framework is flexible and can be expanded for institution specific needs. The last part of the article will demonstrate how the framework can be converted to an model that can be used in an operational sense in the management of security workforce competencies for a specific organization.

THE EBK FRAMEWORK IN WHOLE

The EBK is a fairly short document by design. Many of the details are intentionally left to the implementer, as the document describes a framework rather than act as a prescriptive document. The document is comprised of five sections; Introduction, IT Security Competency Areas, IT Security Key Terms and Concepts, IT Security Roles, Competencies and Functional Perspectives, and the IT Security Roles, Competencies and Functional Matrix. The introduction discusses the history behind the EBK and some of the philosophy used in its development. Rather than define the key terms early, the document introduces the concept of competency areas. Competency areas are a way of breaking the various aspects of security into related groups, such as Data Security, Incident Management and Procurement. The key terms are then grouped by these competencies. Rather than deal with the myriad of job titles, the document has a section on roles, a generic form of job title. Combining roles and competencies, the actionable element of a functional perspective is introduced. The final section is a matrix representation of the relationship between competencies, roles and functional perspectives.

The EBK framework is a structured representation of the relationships between the roles and competencies of the IT security workforce. Roles are a method of describing different IT job positions while avoiding the myriad of job titles for equivalent positions. Roles are grouped into different types; Executive, functional and corollary. IT security competencies represent a generic method of describing different aspects of IT security work functions. At the intersection of a role and a competency is a functional opportunity to achieve specific security results. This intersection is broken into four types of functional perspectives.

IT Security Key Terms and Concepts

In section 3 of the EBK, a listing of key IT security terms and concepts is included to assist the readers with the standard vocabulary used in the description of the roles and competencies. A total of 248 terms are listed in section 3. The purpose of the listing is to provide readers a basic listing of key terms and concepts that should be understood in order to implement aspects of the EBK. Basic knowledge of these terms is needed to appropriately map the EBK to a specific organization.

An IT security generalist or professional should have a solid working knowledge of all of the terms. The terms are listed by technical competency area to facilitate organization. A solid working knowledge of these terms and concepts is foundational for the effective performance of functions associated with each of the technical competency areas. A listing of the terms and definitions will be published as a separate companion document to the EBK.

EBK IT Security Competency Areas

The EBK lists 14 generic IT security competencies that is distilled from a wild range of sources across the IT industry, including the examination of common IT security standards and best practices by a series of subject matter experts (SME). Grouping the functions into 14 generic competencies allows the information to be adopted by organizations without the work of translating and dividing material into a particular organization's design of IT security functionality.

14 IT Security Competency Areas (DHS 2008)

- Data Security
- Digital Forensics
- Enterprise Continuity
- Incident Management
- IT Security Training and Awareness
- IT Systems Operations and Maintenance
- Network and Telecommunications Security
- Personnel Security
- Physical and Environmental Security
- Procurement
- Regulatory and Standards Compliance
- Security Risk Management
- Strategic Security Management
- System and Application Security

EBK IT Security Roles

In an organization, personnel are assigned roles with titles to differentiate responsibilities and duties. The EBK captures this aspect through the definition of a series of roles. These roles have been developed through an examination of a wide variety of IT job titles with IT security responsibilities. The use of roles provides a simple mechanism that allows the EBK to be applied across virtually any enterprise. One of the first tasks that must be performed before using the EBK in a specific organization is the mapping of organization specific jobs to the generic EBK roles.

The roles are split into three groups; Executive, Functional and Corollary. Although these roles may not match any organizations, the tasks associated with the roles can be mapped to virtually any organization. During the mapping function, there may be multiple job titles in an organization that can be mapped to a specific role. This is expected and normal. It is also possible that the role of digital forensic professional may not have anything mapped to it. This makes sense in the light of the highly specialized nature of the role. In the event that this occurs, it is important to examine the contents of this role and ensure that they are adequately covered by the other mapped job titles.

Executive Roles

The three executive roles are probably the easiest to map as they are common in most organizations and are common to be solo in nature. The role of Chief Information Officer occurs in all organizations, although it may be titled as a Vice President position. This is probably the easiest role to map, as every organization has a CIO equivalent. The CIO role is defined as the IT leader of the organization. The executive roles defined in the EBK are Chief Information Officer, Information Security Officer and IT Security Compliance Officer.

The key to determining the mapping is in examining the defining aspects of the role as listed in the EBK and comparing those to the assigned job responsibilities. This approach is used for all remaining job titles, examining the responsibilities and mapping to defined roles in the EBK.

Functional Roles

The vast majority of IT positions will map against the roles listed in the functional role group. These roles represent core information technology roles. The functional roles defined in the EBK are Digital Forensics Professional, IT Security Engineer, IT Security Operations and Maintenance Professional, and IT Security Professional.

The Digital Forensics Professional is a highly specialized role, whereas the IT security professional represents a generalized one. Both technical jobs and operational IT jobs are covered by IT Security Engineer and IT Security Operations and Maintenance Professional respectively. This allows the mapping of most IT job titles to appropriate functional roles.

Corollary Roles

The remaining category is that of Corollary roles, a group that is used to define security responsibilities across typically supportive type IT jobs. The corollary roles defined in the EBK are Physical Security Professional, Privacy Professional, and Procurement Professional.

These roles are important aspects of any IT organization and the responsibilities in these roles should be mapped to appropriate supporting job titles.

Mapping Completeness

After examining all of the roles in the three groups and mapping organization specific job titles to these roles, and examination of completeness is needed. Completeness is the idea that all IT related jobs will be mapped to a role, and all roles will be used in the mapping. There is the possible exception of the forensics role, but if that role is not mapped, the functional elements listed under that role need to be examined and appropriately distributed across other jobs within the organization.

The rationale behind completeness comes from the design of the EBK framework. This framework was developed using a whole host of current security frameworks and designs, including elements of CoBit, ISO 27000 series, the CISSP body of knowledge and a whole host of best practices including those promoted by NIST through their 800 SP series of technical publications. By capturing and extracting the relevant human resource elements of security, the EBK acts as a distillation of best practice laid out in generic form ready for implementation across a wide spectrum of organizations. In adopting or using the EBK, the organization is attempting to benefit from all of this best practice capture and define the appropriate responsibilities across specific job titles and functions. Completeness is merely a mechanism to ensure the task is completed in scope, breadth and depth.

Functional Event Types

The functional events at this intersection can be categorized in four groups; Manage, Design, Implement, and Evaluate. Functional events fall into one of these categories based on the type of activity represented.

- **Manage** functions are those related to management such as overseeing technical and operational activities from the highest levels. These functions ensure security system currency with the changing risk and threat environments.

- **Design** functions are those that relate to the design and development of security related functionality. Included are technical architectural as well as work process design aspects.

- **Implement** functions are those that involve tasks associated with the implementation of operational security measures, including programs, policies and procedures.

- **Evaluate** functions are equivalent to internal audit of security functionality, including activities to assess the effectiveness of policies, procedures, programs or controls in achieving security objectives.

The relationship described by the framework is illustrated in Figure 1.

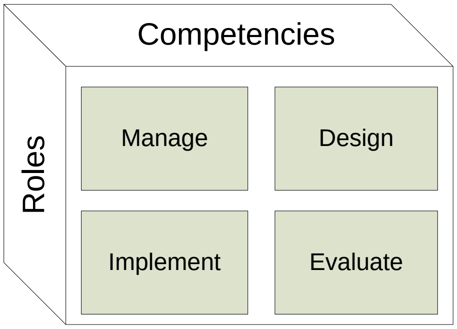

Figure 1. Relationship of Roles, Competencies and Functions (DHS 2008).

The EBK describes ten different roles, from the top of the executive chain (CIO) to basic roles such as IT security professional and corollary roles such as privacy officer. The fourteen competencies include items such as data security, forensics, training and awareness, personnel security, physical security, risk management and application security. Both the roles and the competencies were developed by DHS personnel after examining numerous industry and government specific documents and best practices. Their objective was to create a generic framework that could be adopted by a wide range of government agencies. As such, the document is descriptive in generic terms as the following examples will illustrate.

The juncture of the CIO role and the Enterprise Continuity competency is classified as a Manage function. Example statements from the EBK for this function include:

- Define the enterprise continuity of operations organizational structure and staffing model
- Define emergency delegations of authority and orders of succession for key positions

For the junction of the role of IT Security Operations and Maintenance Professional and the IT Systems Operations and Maintenance competency there are defined examples for all four functions:

Design

- Develop personnel, application, middleware, operating system, hardware, network, facility, and egress security controls
- Develop security monitoring, test scripts, test criteria, and testing procedures

Implement

- Establish a secure computing environment by applying, monitoring, controlling, and managing unauthorized changes in system configuration, software, and hardware
- Collaborate with technical support, incident management, and security engineering teams to develop, implement, control, and manage new security administration technologies

As can be seen from the examples, the EBK is designed to be general in its guidance, leaving the specifics up to the implementers within each organization. Although the EBK was designed using the best sources available at the time of its creation, as time passes and the IT security landscape changes there will be opportunities that necessitate additions to the EBK.

What is not in EBK

The EBK is designed for use across the public and private sectors and topics that are not applicable to the majority of these areas have not been included in the initial version. For example, the certification and accreditation (C&A) process, which is mandated by the Office of Management and Budget (OMB) Circular A-130 and applies only to systems that house Federal data, is not included as a function within a competency. In a similar vein, issues such as the National Security Agency's sponsored work in topics such as Open Vulnerability and Assessment Language (OVAL) and configuration management via Security Technical Implementation Guides (STIGs) are not included as they primarily served a small market compared to the entire IT market. These items can be added into the implementation of the EBK by extending the framework as detailed in the next section.

FRAMEWORK EXPANSION

The EBK framework can be expanded upon in two different dimensions. First, the number of roles and competencies can be expanded. Additional roles can be added for new roles as they become identified through the ever evolving nature of information security operations. New competencies can also be added in the same manner. Figure 2 illustrates an expanded framework with both new roles and new competencies added. The important factor to consider is how this expansion affects the framework, and the answer is simple – not at all. The framework is robust and is designed in such a way that these expansions are natural consequences of the evolving nature of security workforce management.

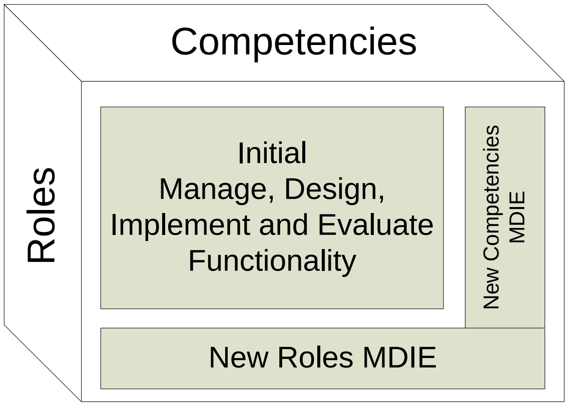

Figure 2. Expansion of EBK through additional roles and competencies

When a new role is being considered for addition to the EBK framework, it is important to remember the separation of roles and job titles. Roles are generic in nature and by design are broad to cover several job titles in different industries. In the case of a firm with a substantial investment in biometrics, they may have individuals that are biometric engineers, whose responsibilities include the design, implementation and maintenance of biometric based security systems. Rather than add a specific role for this type of job, it would be folded under the IT Security Engineer role. The objective is to keep the number of roles to a manageable size to facilitate the simplification afforded by the framework. A good guide to use in this determination is the example provided by the Digital Forensics Professional vs. the IT Security Operations and Maintenance Professional role. The Digital Forensic Professional is a specialist, who job duties exist outside the normal chain of the standard IT security business model. The IT Security Operations and Maintenance Professional is the core work functionary of the standard IT security business model. Separating out the specialist role allows a more complete framework without adding rarely used detail into a common work function area.

Institution Additions

For an institution to properly adopt the EBK there will be specific instances where the EBK as published has missing aspects that are important to the organization. Just as the framework aspect of the EBK allows it to be expanded to add additional roles and competencies, the same framework can be overlaid with an additional layer adding institutional specific elements. This additional layer maintains the same format as the initial EBK layer, with the relationships between roles, competencies and functionalities. Using the framework in this fashion allows a structured method for defining the required aspects of an IT security workforce development plan.

As shown in figure 3, the initial EBK acts as a base layer, and on top of this, institution specific elements are added. The whole diagram, taken together is the specific form of the EBK for a given institution.

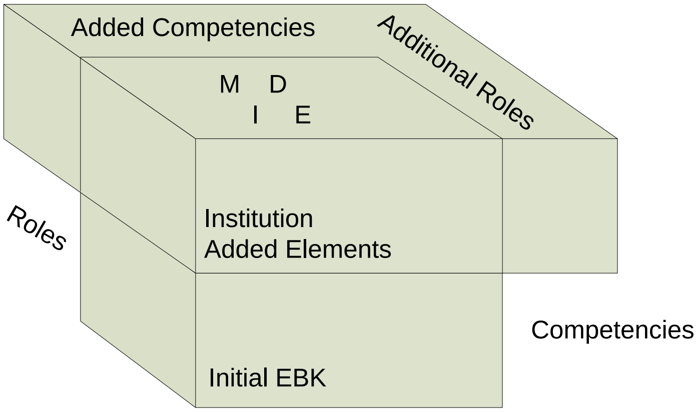

Figure 3. Institutional additions to EBK

Taking the appropriate aspects of the initial EBK and adding the institutional specific elements creates a specific instance of the EBK aligned to an organization. Because of the modular nature of the framework, future subsequent changes can be done as simple delta corrections to previous work. Once the specific instance of the EBK information is created for an institution, the next step is operationalizing the EBK information into specific workforce guidance.

Operationalization

The basis of the EBK is generic information, but for a firm to utilize the information in a meaningful way it needs to be specific. To operationalize the EBK for use in a specific firm or institution requires a translation of the general information into specific information that is relevant to the firm. This is a simple statement by statement translation of the adopted EBK information into specific information relevant to the firm. The following examples show the translation of EBK information into firm specific actionable elements. The EBK form "Develop an enterprise continuity of operations plan and related procedures" becomes "Develop an enterprise continuity of operations plan and related procedures for all IT systems, including outsourced aspects," and "Specify security requirements for the IT system or application" becomes "Specify security requirements for all internally developed or purchased IT systems or applications."

The objective is to turn generic statements into actionable items that can be used by management in IT security workforce planning and development. In this manner, the framework nature of the EBK, coupled with information added by subject matter experts in an organization can be transformed into an actionable planning document. This same information, because of the modular framework nature can be easily updated and maintained in a current state.

CONCLUSION

The IT Security EBK is built directly upon the work of established methods and best practices from both the public and private sectors. The relevant details of these industry wide best practices are directly reflected within the content of the EBK. The EBK is not an additional set of guidelines, and it is not intended to represent a standard, directive, or policy by DHS or any other agency. Instead, it acts to clarify key IT security terms and concepts for well-defined competencies; identifies generic security roles; defines four primary functional perspectives. The EBK acts as a framework defining IT Security Roles, Competencies, and their relationship in a Functional Matrix. This framework aspect of the EBK is one of its strongest benefits, for through this organization the complexities of the wide ranging aspects of IT security functionality can be managed in a reasonably sized form.

People are often faulted as the weakest link in a security implementation (Sasse, Brostoff et al. 2001). Training and education of personnel is frequently the target when results are less than desired. With a complex topic such as IT security multiplied by the complexity of today's networks, the difficulty associated with proper resource allocation was unmanageable. The EBK was designed to provide two key benefits for the professional development and workforce management of personnel with IT security functions.

- Articulate the functions that professionals within the IT security workforce perform, in a format and language that is context-neutral and applicable across a wide array of enterprises in both the public and private sectors.
- Provide content that can be leveraged to facilitate cost-effective and targeted professional development of the IT workforce—including future skills training and certifications, academic curricula, or other affiliated human resource activities.

The very structure and simplifying nature of the EBK reduces the complexity to a manageable scale and also permits the collaboration between different agencies and enterprises through a common reference model.

The EBK can be an outstanding tool for management to use in unraveling the complexities associated with defining the correct job task based training and awareness requirements that align with IT security responsibilities. The framework of the EBK allows the deconstruction of the complexity through a series of mappings of the EBK framework to firm specific job tasks. Proper management of the foundational element of assuring that personnel have the correct training for the job tasks assigned is a key to success. And the EBK has provided firms a great pathway to achieve positive results in the management of this aspect of the IT security endeavor.

The EBK adds value to an organization’s quest for better IT security management. It does this not by adding new requirements, but through the simplification of the complex relationship between roles, characteristics and functional perspectives associated with IT security. The framework described by the EBK separates the complex relationships associated with IT security and functional perspectives into a manageable form. The framework is simple in form, although lengthy to implement, and yet it provides documentable evidence that can be used to manage workforce training issues. By instilling the information from the wide range of sources, and applying them in a simple framework, the EBK adds value to the information security management task. In this respect, it allows managers to use less and get the job done.

Future Direction

The true value of the EBK will be decided by the organizations that adopt and use it. Because it is new, Fall of 2008, it will take time for its adoption and proofing in the marketplace. As the EBK is adopted in Federal agencies in the coming year, research into its effectiveness and completeness in practice will be undertaken.

References

Allenby, B. and J. Fink (2005). *Toward Inherently Secure and Resilient Societies*, American Association for the Advancement of Science. **309:** 1034-1036.

DHS (2008). *Information Technology Security Essential Body of Knowledge: A Competency and Functional Framework for IT Security Workforce Development*. Washington, D.C., Department of Homeland Security - National Cyber Security Division. **September 2008:** 51.

Sasse, M. A., S. Brostoff, et al. (2001). "Transforming the 'weakest link' - a human/computer interaction approach to usable and effective security." *BT Technology Journal* **19**(3): 122-131.

Shaw, R. S., C. C. Chen, et al. (2008). "The impact of information richness on information security awareness training effectiveness." *Computers & Education*.

Theoharidou, M., E. Stougiannou, et al. (2007). *A CBK for Information Security and Critical Infrastructure Protection*, Springer.