Expanding Knowledge in Cyberawareness and Careers in Cybersecurity

It's now clear that this cyber threat is one of the most serious economic and national security challenges we face as a nation. It's also clear that we're not as prepared as we should be, as a government or as a county.

President Barrack Obama, May 29, 2009

We not only have a shortage of the highly technically skilled people required to operate and support systems we have already deployed, we also face an even more desperate shortage of people who can design security systems, write safe computer code, and create the ever more sophisticated tools needed to prevent, detect, mitigate, and reconstitute systems after an attack.

A Human Capital Crisis in Cyber Security, 2010

DECODING THE CYBERSECURITY PROFESSION

For some, CyberSecurity focuses on the technical aspects of computer defense: the safety of computers and computer systems in a networked environment, while Information Assurance (IA) focuses on confidentiality, integrity, availability and validation of data, and therefore CyberSecurity is a subset of Information Assurance. However, others, particularly the Department of Defense, state that IA is a subset of CyberSecurity and CyberSecurity includes management of the risks associated with computers and networks and mission assurance. The CyberWatch K12 Division does not concern itself with the subtleties of the differences; it lives in the intersection of the definitions. We define here CyberSecurity in our context.

It seems that everything relies on computers and the internet now — communication (email, cellphones), entertainment (digital cable, mp3s), transportation (car engine systems, airplane navigation), shopping (online stores, credit cards), medicine (equipment, medical records), and the list goes on. How much of your daily life relies on computers? How much of your personal information is stored either on your own computer or on someone else's system?

The Center for Strategic and International Studies (CSIS) Commission on CyberSecurity fort the 44th Presidency suggests the term "cyber security services" to mean the development, implementation, operation and administration of measures and/or activities intended to prevent, detect, recover from and/or respond to intentional or inadvertent compromises of the confidentiality, integrity and availability of information technology including but not limited to intrusion detection, computer forensics, configuration management, and system development.

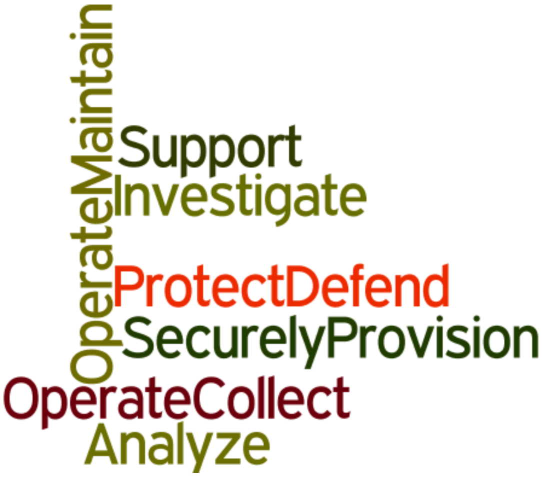
CyberSecurity involves protecting that information by preventing, detecting, and responding to attacks. In the most general terms, it involves protecting data and communications, but fields which may not necessarily fit everyone's definition of cybersecurity may be involved. These include accounting, forensic science, law enforcement, bioengineering, intelligence, communications, management science, systems engineering, criminology, security engineering, computer science, and robotics.

Career *focus*

Seven Categories
31 Specialty Areas

"The National Initiative for Cybersecurity Education (NICE) is a nationally coordinated effort focused on cybersecurity awareness, education, training, and professional development. Two Executive Branch initiatives, in 2008 and 2010, founded the NICE. It seeks to encourage and build cybersecurity awareness and competence across the nation and to develop an agile, highly skilled workforce capable of responding to a dynamic and rapidly developing array of cyber threats".

Cybersecurity Workforce Framework



CyberWatch K12 Division

The CyberWatch K12 Division, led by Educational Technology Policy, Research and Outreach (ETPRO), extends the CyberWatch mission to the K12 Community.

http://www.edtechpolicy.org/cyberk12/

Seven Categories
31 Specialty Areas

SECURELY PROVISION

Specialty areas concerned with conceptualizing, designing, and building secure IT systems, with responsibility for some aspect of the system's development.

Information Assurance Compliance

Oversees, evaluates, and supports the documentation, validation, and accreditation processes necessary to assure that new IT systems meet the organization's IA requirements. Ensures compliance from internal and external perspectives.

(Example job titles: Accreditor; Auditor; Certification Agent; IA Manager; Risk Analyst)

Software Engineering

Develops, creates, and writes/codes computer applications, software, or specialized utility programs.

(Example job titles: Programmer; IA Engineer; Software Developer; Systems Analyst, Web Developer)

Enterprise Architecture

Develops system concepts and works on the capabilities phases of the systems development lifecycle; translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes.

(Example job titles: IS Architect, IS Security Engineer; Network Security Analyst; Systems Engineer; Security Solutions Specialist)

Technology Demonstration

Conducts technology assessment and integration processes; provides and supports a prototype capability and evaluates its utility.

(Example job titles: Capabilities and Development Specialist; R & D Engineer)

Systems Requirements Planning

Consults with customers to gather and evaluate functional requirements and translates these requirements into technical solutions. Provides guidance to customers about applicability of information systems to meet business needs.

(Example job titles: Business Analyst; Contracting Officer; Requirements Analyst; Systems Engineer; Solutions Architect)

Test and Evaluation

Develops and conducts tests of systems to evaluate compliance with specifications and requirements of systems or elements of systems incorporating IT.

(Example job titles: Security Tester; Security Engineer; Quality Assurance Tester; R&D Engineer; Systems Engineer; Testing and Evaluation Specialist)

Systems Development

Works on the Development phases of systems development lifecycle.

(Example job titles: IA Developer; IA Engineer; IS Security Engineer; Program Developer; Security Engineer; Systems Engineer)

OPERATE AND MAINTAIN

Specialty areas responsible for providing the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security.

Data Administration

Develops and administers databases and data management systems that allow for the storage, query, and utilization of data.

(Example job titles: Data Architect; Database Administrator; Database Developer; Dissemination Manger)

Information System Security Management

Oversees the information assurance program of an information system inside or outside the network environment

(Example job titles: IA Manger; IA Security Officer; IS Program Manager)

Knowledge Management

Manages and administers processes and tools that enable the organization to identify, document, and access intellectual capital and information content.

(Example job titles: Business Analyst; Intelligence Manager; Information Owner)

Customer Service and Technical Support

Addresses problems, installs, configures, troubleshoots and provides maintenance and training in response to customer requirements or inquires

(Example job titles: Support Specialist; Desk Support)

Network Services

Installs, configures, tests, operates, maintains, and manages networks and their firewalls, including hardware (hubs, bridges, switches, routers, cables, proxy servers, and protective services) and software that permit the sharing and transmission of all spectrum transmissions of information to support the security of information and information systems.

(Example job titles: Cable Technician; Network Engineer; Network Administrator; Network Systems Analyst; Telecommunication Engineer)

System Administration

Installs, configures, troubleshoots, and maintains server configurations (hardware & software) to ensure their confidentiality, integrity, and availability Also maintains accounts, firewalls, and patches. Responsible for access control/passwords/account creation and administration.

(Example job titles: LAN Administrator; Server Admin; Systems Operations; Website Admin)

Systems Security Analysis

Conducts the integration/testing, operations, and maintenance of system security

(Example job titles: IA Operational Engineer; IA Security Officer; IS Security Engineer; Security Administrator; Security Analyst; Security Control Assessor)

PROTECT AND DEFEND

Specialty areas responsible for the identification, analysis, and mitigation of threats to internal IT systems or networks.

Computer Network Defense

Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur within the network in order to protect information, information systems, and networks from threats.

(Example job titles: CND Analyst (Cryptologic); Cyber Security Intelligence Analyst; Incident Analyst; Network Defense Technician; Security Analyst; Security Operator)

Incident Response

Responds to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.

(Example job titles: Computer Crime Investigator; Incident Handler; Incident Responder; Intrusion Analyst)

Computer Network Defense Infrastructure Support

Tests, implements, deploys, maintains, and administers the infrastructure hardware and software that are required to effectively manage the computer network defense service provider network and resources. Monitors network to actively remediate unauthorized activities.

(Example job titles: IDS Admin; IDS Engineer; IDS Technician; IS Security Engineer; Network Admin; Network Security Specialist; Security Specialist)

Security Program Management

Manages relevant security implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, policy enforcement, emergency planning, security awareness, and other resources

(Example job titles: Chief Information Security Officer (CISO); Common Control Provider; Enterprise Security Officer; Facility Security Officer; IT Director; Risk Executive

Vulnerability Assessment and Management

Conducts assessments of threats and vulnerabilities, determines deviations from acceptable configurations, enterprise or local policy, assesses the level of risk, and develops and recommends appropriate mitigation countermeasures in operational and non-operational situations.

(Example job titles: Blue Team; CND Auditor; Compliance Manager; Ethical Hacker; Governance Manager; Penetration Tester; Red Team; Reverse Engineer; Risk Manager)

```
#pragma once
#endif // _MSC_VER > 1000
#ifndef __AFXWIN_H__
        #error include [illegible]
#endif
#include "resource.h"      // [illegible]
// CDMotionApp:
// See DMotion.cpp for the [illegible]
//
class CDMotionApp : public [illegible]
{
public:
        CDMotionApp();
// Overrides
        // ClassWizard [illegible]
        //{{AFX_VIRTUAL([illegible]
        public:
        virtual BOOL [illegible]
        //}}AFX_VIRTUAL

// Implementation
        //{{AFX_MSG([illegible]
        afx_msg void [illegible]
            // NOTE - the [illegible]
            //    DO NOT EDIT [illegible]
```

INVESTIGATE

Specialty areas responsible for the investigation of cyber events and/or crimes of IT systems, networks, and digital evidence.

Investigation

Applies tactics, techniques, and procedures for a full range of investigative tools and processes to include, but not limited to, interview and interrogation techniques, surveillance, counter surveillance, and surveillance detection, and appropriately balances the benefits of prosecution versus intelligence gathering.

(Example job titles: Computer Crime Investigator; Special Agent)

Digital Forensics

Collects, processes, preserves, analyses, and presents computer-related evidence in support of network vulnerability mitigation, and/or criminal, fraud, counterintelligence, or law enforcement investigations.

(Example job titles: Computer Network Defense Forensic Analyst; Digital Forensic Examiner; Digital Media Collector; Forensic Analyst; Cryptologist; Network Forensic Examiner)

OPERATE AND COLLECT

Specialty areas responsible for the highly specialized collection of cybersecurity information that may be used to develop intelligence

Collection Operations

Executes collection using appropriate strategies and within the priorities established through the collection management process

Cyber Operations Planning

Gathers information and develops detailed Operational Plans and Orders supporting requirements. Conducts strategic and operational level planning across the full range of operations for integrated information and cyberspace operations.

Cyber Operations

Uses automated tools to manage, monitor, and execute large-scale cyber operations in response to national and tactical requirements.

ANALYZE

Specialty areas responsible for highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence

Cyber Threat Analysis

Identifies and assesses the capabilities and activities of cyber criminals or foreign intelligence entities; produces findings to help initialize or support law enforcement and counterintelligence investigations or activities.

Exploitation Analysis

Analyzes collected information to identify vulnerabilities and potential for exploitation.

Targets

Applies current knowledge of one or more regions, countries, non-state entities, and technologies

All Source Intelligence

Analyzes threat information from multiple sources, disciplines, and agencies across the Intelligence Community. Synthesizes and places intelligence information in context; draws insights about possible implications

SUPPORT

Specialty areas providing support so that others may effectively conduct their cybersecurity work.

Legal Advice and Advocacy

Provides legally sound advice and recommendations to leadership and staff on a variety of relevant topics within the pertinent subject domain. Advocates legal and policy changes and makes a case on behalf of client via a wide range of written and oral work products, including legal briefs and proceedings.

(Example job titles: Legal Advisor/SJA)

Strategic Planning and Policy

Development

Applies knowledge of priorities to define an entity's direction, determine how to allocate resources, and identify programs or infrastructure that are required to achieve desired goals within domain of interest. Develops policy or advocates for changes in policy that will support new initiatives or required changes/enhancements.

(Example job titles: Chief Information Officer (CIO); Command IO; Information Security Policy Analyst; Information Security Policy Manager; Policy Writer)

Education and Training

Conducts training of personnel within pertinent subject domain. Develops, plans, methods, and techniques as appropriate.

(Example job titles: Cyber Trainer; IS Trainer; Security Training Coordinator)