Cybersecurity: It Only Takes Seconds For a Hacker To Take EVERYTHING

Anne Kohnke, PhD; Veera Raghava Prasad Govinda Raju (GRA), and Michael Bruno Selvaraj

College of Business + Information Technology, MSIT Program

INTRODUCTION

What is Cybersecurity?

The Internet age has produced a lot of jargon and one of those is the term "cybersecurity." A few of the examples of attempts to define cybersecurity by researchers and IT security professionals are as follows:

- Cybersecurity involves human intelligence—exploits and vulnerabilities are created to defy and change the rules of systems they target (Toecker 41).
- Cybersecurity is nongeographical, it is epiphenomenal and a consequence of the computer and Internet revolution and a problem unlike any other security problem the nation has faced before (Harknett and Stever 455).
- Cybersecurity tends to be used as a synonym for information systems security encompassing identity and access management, breach incident response and the protection of information technology infrastructure such as networks, routers, email, and Web servers (Bissell 38).

Although there are many definitions, **the one thing hackers target is information in the form of electronic data and the aim for organizations is protection.** Cybersecurity is a relatively new discipline, and the absence of a common language to discuss and understand the work and skill requirements hinders the nation's ability to baseline capabilities, identify skill gaps, develop talent in the current workforce, and prepare the pipeline of future talent.

Several challenges are identified: A lack of a standardized language to describe and organize cybersecurity work; Lack of college programs that clearly align to cybersecurity jobs; Employer training and retraining of new hires in the specific skills required; Unclear job prospects and career opportunities for students; and The need for policy makers to set standards that promote workforce professionalization.

In an effort to increase cybersecurity awareness in general, promote cybersecurity instruction in secondary and higher education, and improve development of a cybersecurity workforce, the National Institute of Standards and Technology (NIST) has created the National Initiative on Cybersecurity Education (NICE) *National Cybersecurity Workforce Framework.* The *Cybersecurity Workforce Framework* provides a working taxonomy intended to fit into an organization's existing occupational structure in both the private and public sectors (NIST).

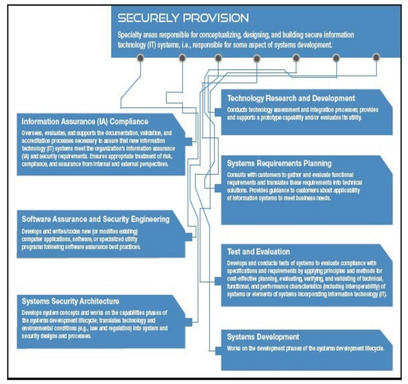
NICE Cybersecurity Workforce Framework Categories

NATIONAL CYBERSECURITY WORKFORCE FRAMEWORK
Specialty Areas of Knowledge for Cybersecurity

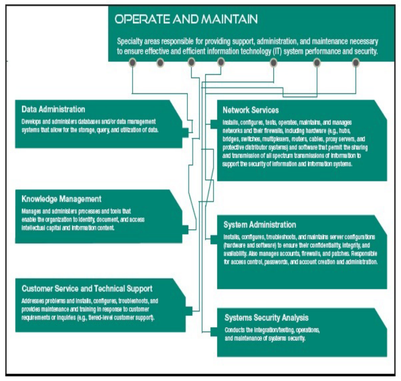
The *Cybersecurity Workforce Framework* established a common taxonomy and lexicon that is used to describe all Cybersecurity work and workers irrespective of where or for whom the work is performed. Its stated aim is to completely and correctly define all of the roles in the cybersecurity workforce and to provide a set of standardized terms for use in cybersecurity work. The *Cybersecurity Workforce Framework* is based on "Categories", "Specialty Areas" within the workforce, and the requisite "Knowledge Skills and Abilities" for each specialty area.

What kinds of skills and abilities are needed for cybersecurity work?

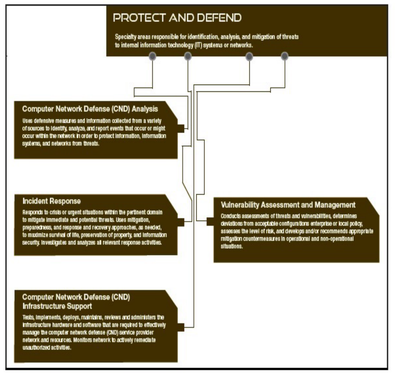
The *Cybersecurity Workforce Framework* identifies and defines 32 specialty areas of cybersecurity work under the umbrella of 7 categories:



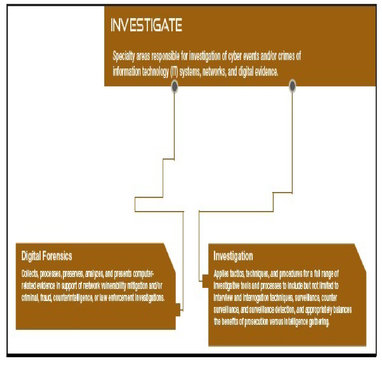
SECURELY PROVISION - Specialty areas responsible for conceptualizing, designing and building secure information technology (IT) systems (i.e., responsible for some aspect of systems development).



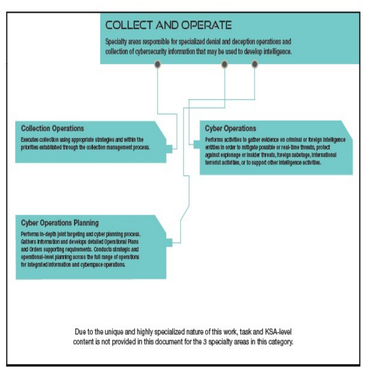
OPERATE AND MAINTAIN - Specialty areas responsible for providing support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security systems development).



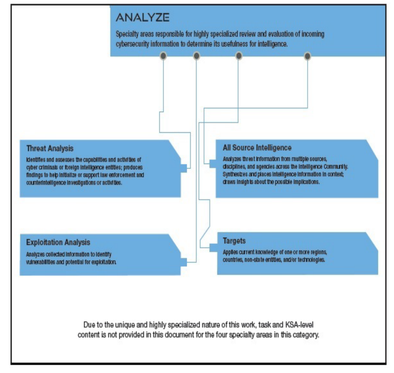
PROTECT AND DEFEND - Specialty areas responsible for identification, analysis, and mitigation of threats to internal information technology (IT) systems or networks.



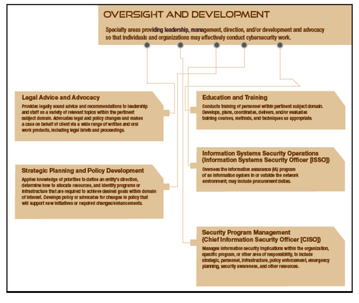
INVESTIGATE - Specialty areas responsible for investigation of cyber events and/or crimes of information technology (IT) systems, networks, and digital evidence.



COLLECT AND OPERATE - Specialty areas responsible for specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.



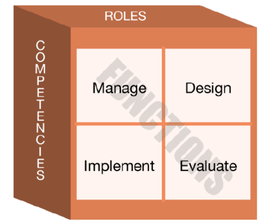
ANALYZE - Specialty areas responsible for highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.



OVERSIGHT AND DEVELOPMENT - Specialty areas providing leadership, management, direction, and/or development and advocacy so that individuals and organizations may effectively conduct cybersecurity work.

COMPETENCIES

The *IT Security Essential Body of Knowledge (EBK)* provides a comprehensive overview of **14 competency areas** for **ten security professional roles** within an organization.



IT Security EBK: 14 Competency Areas:
Data Security, Digital Forensics, Enterprise Continuity, Incident Management, IT Security Training and Awareness, IT Systems Operations and Maintenance, Network Security and Telecommunications, Personnel Security, Physical and Environmental Security, Procurement, Regulatory and Standards, Risk Management, Strategic Management System and Application Security

Key Terms and Concepts:
Assessment, Auditing, Certification, Compliance, Ethics, Evaluation, Governance, Laws, Policy, Privacy Principles/Fair Info Practices, Procedure, Regulations, Security Program, Standards, Validation, Verification

IT Security EBK: 10 Roles
Chief Information Officer (CIO), Digital Forensics Professional, Chief Information Security Officer (CISO), IT Security Compliance Professional, IT Security Engineer, IT Systems Operations and Maintenance Professional, .IT Security Professional, Physical Security Professional, Privacy Professional, Procurement Professional

CYBERSECURITY TOOLS

http://www.cyber50.org/tools --Cybersecurity Tools page

NMAP-Network Mapper is used to discover hosts and services on a computer network, thus creating a "**map**" of the **network**.

Nessus- is a remote security scanning tool, which scans a computer and raises an alert if it discovers any vulnerabilities that malicious hackers could use to gain access to any computer connected to a network.

Metasploit- Audit verification tool and vulnerabilities detection tool.

Armitage—Data encryption and decryption tool for communication. Used for data encryption and decrypting text, email, files, directories and whole disk partitions.

The greatest cybersecurity tool is your **mind**—Train yourself and never stop learning.

Works Cited (MLA)

Bissell, Kelly. "A Strategic Approach to Cybersecurity." *Financial Executive* 29.2 (Mar 2013):36-41. Business Source Complete. Web. March 2015.
Harknett, Richard J., and Stever, James. A. "The New Policy World of Cybersecurity." *Public Administration Review* 71.3 (May/Jun 2011): 455-460. Business Source Complete. Web. April 2015.
NIST-National Institute of Standards and Technology. "The National Cybersecurity Workforce Framework 2.0." (April 2014). Web. Nov 2014.
Toecker, Michael. Generation Cybersecurity: What You Should Know, and Be Doing About It. *Power* (2014): 40-45. Business Source Complete. Web. April 2015.