Competency Models In Action:

College Uses Cybersecurity Competency Model to Align and Create Curricula

January 2015

- Addressing the needs of cybersecurity employers and workforce
- Using the Cybersecurity Competency Model to validate existing curricula
- Developing new curricula to align with the Cybersecurity Competency Model

Introduction

We rely on computer systems to help us in virtually all aspects of our lives…at home, in our business, in government, and as part of our national defense efforts. It is vital that those computer systems be protected from those who would steal the information stored on, or seek to sabotage, those systems. It is the job of the cybersecurity expert to ferret out the weaknesses in our systems, and design and implement protective measures.[1]

The National Cybersecurity Institute (NCI) at Excelsior College is dedicated to assisting government, industry, military and academic sectors meet the challenges in cybersecurity policy, technology and education through a variety of initiatives. NCI uses the U.S. Department of Labor, Employment and Training Administration's (ETA) Cybersecurity Competency Model throughout its cybersecurity program, both as a benchmark in evaluating current curricula and as a guidepost in developing new coursework.

The Workforce Need

Employment of information security analysts is projected to grow 37 percent from 2012 to 2022, much faster than the average of all occupations. In 2012, 75,100 individuals were employed in this occupation; in 2022, it is estimated that number will reach 102,500.[2]

Driving a high demand for information security analysts, the frequency and sophistication of cyberattacks have grown over the last few years and many organizations are behind in their ability to detect these attacks. Analysts will be needed to come up with innovative solutions to prevent hackers from stealing critical information or creating havoc on computer networks.[3]

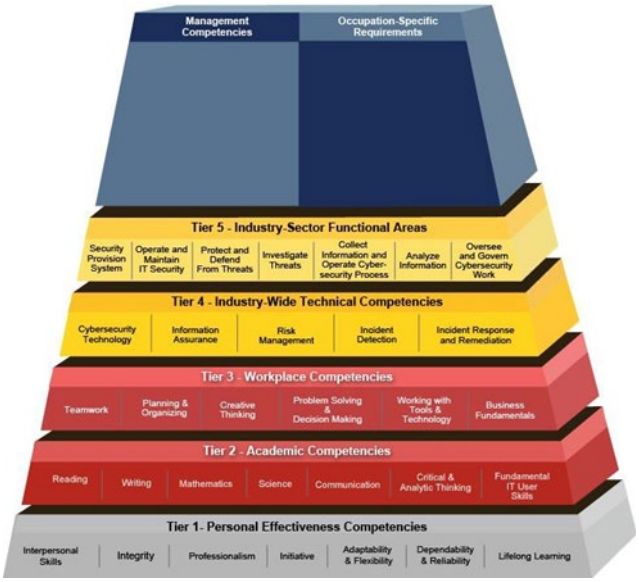
The federal government is expected to greatly increase its use of information security analysts to protect the nation's critical information technology systems. In addition, as the healthcare industry expands its use of electronic medical records, ensuring patients' privacy

[1] http://news.excelsior.edu/excelsior-college-launches-national-cybersecurity-institute/
[2] U.S. Department of Labor, Bureau of Labor Statistics, Occupational Outlook Handbook, 2014-2015 Edition
[3] Ibid

and protecting personal data are becoming more important. More information security analysts are likely to be needed to create the safeguards that will satisfy patients' concerns.[4]

Validation of Existing Curricula

"We are committed to utilizing a curriculum that addresses the needs of cybersecurity employers as well as incumbent and prospective workers," says Dr. Jane LeClair, Chief Operating Officer at NCI and a participating subject matter expert in the development of ETA's Cybersecurity Competency Model. "The sector is unique. For example, a cybersecurity manager will not communicate in normal 'business speak.' At the end of the day, leadership has to understand that the manager was successful in eliminating a threat rather than producing a product."



Key aspects of the foundational tiers of the model are incorporated in most of Excelsior's cybersecurity coursework.

- Tier 1, Personal Effectiveness Competencies: Every course requires interpersonal communication, sets specific expectations for professionalism and personal integrity, as well as an openness and desire to continue to learn and grow.

- Tier 2, Academic Competencies: The entire curriculum builds on the student's existing skills while strengthening and evolving those skills in reading, writing, math, science, communication, critical and analytical thinking and fundamental IT user skills.

- Tier 3, Workplace Competencies: All of these competencies are incorporated into every course including enhancing the student's planning and organization,

Design of New Curriculum

"Excelsior College has developed a new course, Network and Application Security, which focuses on Tiers 4 and 5 of the Cybersecurity Competency Model," says Dr. Denise Pheils, an NCI Fellow. "This course addresses key skills in Tier 4, Industry- Wide Technical Competencies, through its focus on cybersecurity tools and systems and many of the critical

[4] Ibid

work functions under Information Technology Architecture, Operational Technology, Networks and Security Technology Awareness."

The course will cover the fundamental concepts of network and application security. It will equip learners with the technical and conceptual skills required to secure and defend computer networks in organizations. Learners will analyze network security threats and lean to configure and manage network security devices such as firewalls, intrusion detection and prevention systems. The course will also cover elements of web security, wireless security and application security.

Next Steps

"Workers in the cybersecurity field need to commit to the concept of lifelong learning as reflected in the Personal Effectiveness Competencies," says Dr. LeClair. "They will be gaining knowledge on a daily basis. Similarly, as the industry grows, the Cybersecurity Competency Model will continue to evolve. We envision using the model on an ongoing basis as a resource in refining Excelsior College's cybersecurity programs."

Related Links

Excelsior College
http://www.excelsior.edu/programs/technology

National Cybersecurity Institute at Excelsior College
http://www.nationalcybersecurityinstitute.org