GENBERAL BACKGROUND

Marquette University has a M.S. degree program with a specialization in Information Assurance and Cyber Defense. We have recently established a Center for Cyber Security Awareness and Cyber Defense which has goals of education, active community involvement, and research.

Our campus program is distinguished by efforts to work across disciplines to determine appropriate curriculum content about cyber security. Our efforts will span developing cyber security professionals, educating the future technical workforce with awareness of cyber threats and defenses, and instructing other professionals in non-technical disciplines so that they are prepared to address cyber security issues in their chosen profession.

In our community involvement, we work with the local business community as well as nonprofit organizations in the community as well as governmental organizations to offer a variety of efforts that span everything from the very technical issues to awareness for the general population. We will also partner with other academic institutions 2-yr and 4-yr to share knowledge and events.

Our research involves technical development, technology analysis, understanding best-practices, and developing curriculum for a variety of professions.

GROWING AND SUSTAINING

1. As a member of the NICE academic working group, I am aware of the evolving understanding of education, training, and workforce development activities. The results emerging from the NICE working groups should serve to provide guidelines for metrics and improvements.

2. The NIST workforce framework has supplied the basis for categorization of the work force. While estimates of shortages in the workforce abound, specific shortages in categories and roles should be collected and disseminated as part of the task force being formed.

3. Our center on campus and our IT organization is working to involve all students and faculty in the development of cyber security awareness. This broad reach is important since people are targets and too many professionals handling data that needs security are unaware of the threats and defenses.

4. Large employers and government organizations are beginning the process of adapting the NICE Workforce Framework but this is not yet generally known by the business community. Employers are uncertain what skills they need, which are in short supply, or how to construct job descriptions for what they need. Internal education programs are missing and leaders in many organizations lack an understanding of where to start. Cyber security awareness efforts are nascent in most organizations.

5. The effective education and workforce development programs must be as diverse as the categories, roles and skills found in the NIST Workforce Framework. Since colleges and universities are mandated to have assessment plans, it is these plans that ought to drive an understanding of what is effective. While certification exams exists, there is not a commonly

held belief in the certifications that result. The costs of these certifications is a barrier for many to proceed with certification.

At Marquette, in our M.S. Computing program, we offer an option (COSMIC-Change Opportunity Start, MS in Computing) that enables a career transition from a non-technical degree into a technical career. This program was selected by NSF as an element of their S-STEM (scholarships for STEM education) effort. Workers with undergraduate degrees in another field of study are a largely untapped pool of candidates to begin careers in cybersecurity. Working with the Milwaukee area workforce development board a few years ago we discovered almost 300 unemployed workers with a bachelor's degree in Milwaukee County. With limited scholarship offers we have enabled a small number of students to make the career transition.

Conventional 2-yr and 4-yr programs must be an element of growing the workforce, but including career transition efforts at the MS level ought to also be fostered. Employer sponsored efforts can make this a reality. Employers can establish mentorship programs and use education opportunities that foster career change to funnel employees into cyber security careers. While we do this at the baccalaureate to masers level, the concept can be grown and spread. For example, high school graduates could be transition to 2-yr associates' degrees or technical certifications and beyond. High wages, national need, and employer shortfalls can be motivation for establishing robust programs at all levels.

6. The greatest challenges in the workforce are identifying, recruiting, and training a skilled workforce. Skills must be organizational as well as technical. The opportunity lies in insuring that all potential workers with the aptitude and spirit of dedication receive the motivation to move into a cyber security career. While higher wages is working as a motivator, cost of education and even lesser costs such as certification are barriers to entry.

7. New technology can be used by both the defenders and the aggressors making the future uncertain. The cyber security workforce of the future must include all workers. We know that people are the weak link in our defenses. Workforce development must include efforts to span the workforce. So while there are workers with title, roles, and responsibilities dedicated to cybersecurity, all workers must be informed about the threats and defenses; both generally applicable and job specific knowledge must be disseminated.

8. Programs should include awareness, mentorship, apprenticeships, and formal education. Industry specific best practices should be studied. Recommendations should evolve from that and lead to assistance in implementation. NIST has been a leader in a broad sense, but industry groups need to take a role in providing guidance within their industry. Recently we worked with members of a water treatment and deliver industry group. They are aware of the need to develop policies and programs but are unaware of how to start. In a recent panel discussion we sponsored working with K-12 schools systems we discovered a need for efforts in general awareness, career awareness, and career preparedness. Working with specific groups can lead to understanding appropriate measures.