Request for Information: Cybersecurity Workforce, Education, and Training

Background information:

1. **Are you involved in cybersecurity workforce education or training (e.g. Curriculum-based programs)? If so, in what capacity?**

Florida State University's College of Criminology and Criminal Justice is home to one of the nation's top criminology programs. Our faculty are ranked number one in the nation in research productivity and are among the top ten in grant acquisition. Many of our faculty are experts on subjects like gun control, juvenile justice, corrections, biosocial criminology, and social control, to name a few. In addition, faculty have published nearly 1,000 peer-reviewed journal articles, co-authoring many with current and former graduate students.

Students at Florida State University can earn a bachelor's or master's degree in Computer Criminology. This collaborative program includes such courses as Network Security and Cryptography, Computer Security, Cybercrime Detection and Forensics, and Criminal Justice System Responses to Cybercrime.

The criminology program is renowned for its rigorous research, challenging coursework, and inspiring intellectual community. Its academic programs rank among the top in the world and empowers students to develop their interests, express their ideas, and experience the pride of uncovering new knowledge. College graduates possess independent critical-thinking skills honed by policy-informing research, collaborative studies, and leadership engagement opportunities.

The College is committed to applying research and academics to expand the influence of scholarship in the public policy arena and promote evidence-based criminal justice policy and practice at the local, state and national levels. To that end, the Center for Criminology and Public Policy Research supports research initiatives, data collection, and analysis focused on cybercrime, cyber security, and criminal justice policies. The Center maintains relationships with several federal, state, and local agencies in crime prevention, correctional education and reentry, juvenile justice, and other criminal justice areas. In addition, The Center provides graduate students with training to be tomorrow's leaders in criminal justice research and policy.

Growing and Sustaining the Nation's Cybersecurity Workforce:

2. **What current metrics and data exist for cybersecurity education, training, and workforce developments? What improvements are needed in the collection, organization, and sharing of information about cybersecurity education, training, and workforce development programs?**

The United States does not currently have any metrics or datasets regarding cybersecurity education, training, or workforce development. The first suggested step for improvement would be to establish interdisciplinary academic partnerships with criminal justice stakeholders to collect, organize, and evaluate information about cybersecurity education, training, and workforce development programs. Furthermore, the criminal justice community lacks a coherent knowledgebase concerning cybersecurity. For example, no nation-wide, consistent, agreed-upon definition of what is meant by the term "cybersecurity" exists. Nor do we have widespread consensus on education, training, or workforce development requirements. Although "cyber" is often used to describe actions involving a computer, virtual reality, or networks, it is also used as a descriptive term surrounding the categorization of a criminal act. While others have suggested that cybersecurity refers to a collection of acts related to computer based crime. Inconsistent definitions of cybersecurity have important impacts not only for criminologist, but for law enforcement as well, as it may impact how laws are designed, investigated, and how the nation's security of our digital resources is maintained (Taylor, Fritsch, & Liederbach, 2015).

Furthermore, the explosive growth in technology over the past 40 years, together with underdeveloped datasets and metrics have resulted in cybersecurity policies being implemented without empirical support, generalizability, and validity. No systematic datasets are currently available for research regarding cybercrime, cyberterrorism, or cybersecurity, resulting in a lack of understanding on the development, categories, and laws surrounding cybercrime and cybersecurity (Taylor, Fritsch, & Liederbach, 2015). Universities and government programs should seek to collect, organize, and share empirical datasets regarding cybersecurity education, training, and workforce development. In fact, Florida State University's College of Criminology and Criminology Justice is among the first to begin efforts geared towards creating a well-rounded empirical dataset regarding cybersecurity and cybercrime. Future funding and interdisciplinary encouragement could facilitate a nationwide empirical database to enable further cybersecurity exploration efforts.

3. Is there sufficient understanding and agreement about workforce categories, specialty areas, work roles, and knowledge/skills/abilities?

As mentioned, there is a lack of agreement concerning basic definitions of cybersecurity workforce categories, specialty areas, work roles, and knowledge/skills/abilities (Booz, et al., 2015). This lack of definition not only hampers standard practices and laws, but also results in a lack of data consistency. The United States government is not currently aware of the number of cybersecurity employees they have, their skills, or tasks and results in a lack of certainty regarding the direction of cybersecurity (Booz, et al., 2015).

At the Florida State University College of Criminology and Criminal Justice, we believe this gap can be closed through development of an interdisciplinary program and data repository surrounding cybercrime and cybersecurity. The intent behind this program and data repository is to provide the nation's cybersecurity workforce with standard definitions of cybercrime and cybersecurity, and information on how to develop evidence-based cybersecurity policies.

A gap also exists in cybersecurity training at the tactical level. These missing tactical skills and knowledge are needed to effectively prepare for and prevent threats to cybersecurity infrastructure. Per Pelfrey & Pelfrey (2010), there is no clear consensus on what a cybersecurity curriculum should include. Cybersecurity remains disorganized as an academic discipline, and has an uncertain connection to more established disciplines and related fields, such as IT security and engineering. Future cybersecurity programs should focus on an interdisciplinary approach, and should incorporate aspects of other fields to accomplish the unique goal of protecting the nation's businesses, data, and citizens.

4. Are appropriate cybersecurity policies in place in your organization regarding workforce education and training efforts and are those policies regularly and consistently enforced?

Cybersecurity will be made more secure by working with public and private sector partners to build a more resilient cyber infrastructure and developing cyber law enforcement (Taylor, Fritsch, & Liederbach, 2015). Without a consistent definition of cybersecurity and an empirical dataset regarding cybercrime and cybersecurity, academics and law enforcement have difficulty determining whether cybersecurity policies are effective. Due to the lack of empirical research, we are left with relying upon anecdotal evidence to determine if cybersecurity education and training is enforced or effective. The limited research surrounding cybersecurity often relies on small sample sizes, self-report surveys, and data collected by cybersecurity vendors (Taylor, Fritsch, & Liederbach, 2015). In addition, the difficulty in accurately calculating types, motivations, and estimations of cybersecurity breaches results in estimates that vary dramatically. Facilitating these varied estimates, current cybersecurity research efforts typically rely on voluntary compliance by businesses or individuals, resulting in underestimates of cybersecurity breaches (Taylor, Fritsch, & Liederbach, 2015). A recent Florida Department of Law Enforcement study surveyed 898 public and private sector organizations that use computers, and found that 35% of them reported being victimized by computer criminals. However, no attempts to estimate losses were made due to the assumption that the losses would only be a "guess".

Although we know that the costs of cybersecurity breaches are extensive, there is no true estimate of the actual losses due to such breaches or other cybercrime. Therefore, it is vital that researchers and policy makers work together to measure cybersecurity incidents and their impacts. A considerable amount of time, energy, and resources are spent on cybersecurity protection, but no statistically accepted metrics exist to gauge effectiveness of current cybersecurity workforce efforts, education and training policies, or to determine if policies are being enforced. Future efforts should be made to establish datasets that will allow for the evaluation of current cybersecurity education and training policies.

5. Which are the most effective cybersecurity education, training, and workforce development programs being conducted in the United States today? What makes those programs effective? What are the goals for these programs and how are they successful

in reaching their goals? Are there examples of effective/scalable cybersecurity, education, training, and workforce development programs?

As of 2015, there existed no government-wide attempt to build a knowledgeable, trained, and skilled cybersecurity workforce (Booz, Allen, & Hamilton, 2015). This resulted in a nationwide shortage of cybersecurity experts, especially for government organizations. However, universities can attempt to establish a student pipeline by incorporating informed theoretical research to the field of cybersecurity. Additional research should be done in the area of cybersecurity to determine the best ways to combat threats and prepare a knowledgeable cybersecurity workforce. We believe that the first step to a successful cybersecurity program is ensuring that all education and training is rooted in empirical research. To achieve this goal, a comprehensive data repository of cybersecurity and cybercrime should be established. This extensive data repository would be constructed from original qualitative data, multiple sources, and multiple sites, and could be used to predict the types of services, infrastructures, and procedures needed to respond to future incidents of cybercrime. Few studies and data exist for meaningful meta-analyses from which to identify evidence-based best practices for response and recovery to cybercrime and cyberterrorism. Rather methods must include original data collection from primary sources, database construction, and identification of patterns across cases and over time. The second goal is to assess patterns in cybersecurity response and recovery based on research and analysis. Third, conducting gap analysis of cybersecurity education and training may reveal important insight into gaps in cybersecurity knowledge. This assessment would include evaluation of gaps in infrastructure, personnel, and procedures. Finally, such rigorous academic analysis will inform recommendations for evidence-based policies and practices.

6. **What are the greatest challenges and opportunities facing the Nation, employers, and workers in terms of cybersecurity education, training, and workforce development?**

The greatest challenges facing the nation and cybersecurity experts are rooted in the lack of theoretical development and research to guide policies and procedures. The field of cybersecurity in the U.S. tends to favor applied research over informed theoretical research. As a result of this coupled with the exponential growth in technology, the cybersecurity field constantly finds itself unprepared for new forms of cybercrimes and cybercriminals. As research developed on cybersecurity and cybercrime, themes and classifications developed and resulted in a call for the creation of dedicated computer crime units (Taylor, Fritsch, & Liederbach, 2015). Despite these computer crime units, researchers are still often limited to case studies to determine the influence, cause, and risk factors associated with cyber-victimization or cyber-offending. Reliance on case studies, small sample sizes, and introductory college courses as the sample, results in a lack of generalizability to general cybersecurity issues.

Due to the rapid growth in technology, cybersecurity efforts often lack empirical research before implementation, effectiveness is therefore unknown. Excitement for technological advancement is thus clouded by the risk that the new technology will be used for criminal or terroristic ends.

7. What steps or programs should be continued, modified, discontinued, or introduced to grow and sustain the Nation's cybersecurity workforce, taking into account needs and trends? What steps should be taken:

Cybersecurity is very much an emerging field with very diverse approaches informed by numerous disciplines. Some might argue that it lacks a strong theoretic perspective and has yet to become an established academic discipline. Therefore, the field of cybersecurity has two options: it can remain practitioner based like emergency management or it can become theoretically and research driven, ultimately establishing itself as a strong academic discipline. Cybercrime represents a new issue for individuals, government, academic, and business institutions; combatting and preventing it will demand the best collaborative efforts of researchers, policy makers, and practitioner.