# DEVELOPING CYBERSECURITY PROFICIENCY IN AN ERA OF ACCELERATING CHANGE: UTILIZING A BACHELOR DEGREE FOUNDATION FOR EMERGING PROFESSIONALS

A paper submitted to the Commission on Enhancing National Cybersecurity

by George M. Schwartz, Ed.D. (a.b.d.)

Immaculata University

Any organization, public or private, that is networked to the internet has the potential to be targeted by hackers and cyber criminals. The most common attacks are malicious code, denial of service attacks, and web-based intrusions. The typical large American organization loses almost $6 million a year to cybercriminals. On average, it takes such an organization 18 days and hundreds of thousands of dollars to resolve an attack (Perry, 2012).

Unfortunately, the demand for cybersecurity professionals is exceeding the number available, and some estimate that more than 200,000 positions are currently unfilled (Setalvad, 2015). The Bureau of Labor Statistic forecasts the need for cybersecurity professionals increasing by more than 22%, adding more than 27,000 new positions through 2020; a rate much higher than most jobs (retrieved from http://www.bls.gov/ooh/).

## Fulfilling the Demands for Cybersecurity Professionals

What is the best way to develop cybersecurity professionals to reduce the gap between the demand and supply, and what is the role of higher education in helping to meet future needs? A good starting point is to better understand the current skillsets of cybersecurity professionals. This is an analytical challenge since specialties in the field are varied from security generalists to more technical subject expertise such as forensics and penetration testing, although the National Initiative for Cybersecurity Careers and Studies has developed a general framework for knowledge, skills, attributes (2014). Further complicating benchmarking, the education levels of today’s successful cybersecurity professionals are varied; some are self-taught and have not earned a college degree, while others have doctorate degrees, (Morgan, 2016; SANS, 2014).

Today’s cybersecurity leaders agree that higher education is important (SANS, 2014), and efforts by the Obama administration to increase student participation in STEM (Science, Technology, Engineering, Mathematics) programs and emphasizing cybersecurity education as a major part of its Comprehensive National Cybersecurity Initiative, provide a solid foundation for the nation’s future requirements (Lemos, 2013). But education alone is not sufficient. Possessing technical certifications—in such areas as cybersecurity tools, information security, and network engineering—is becoming increasingly the most important factor in career success (Burning Glass, 2016; SANS, 2014). The potential challenge with certifications is, however, that accelerating changes in technology could make current certifications obsolescent.

## A Different Path

The future of cybersecurity is not limited to certifications and technical specialties though. The field is open to professionals with diverse backgrounds who have a firm grounding in security (Lemos, 2013). San José State University President Dr. Mohammad H. Qayoumi, Chairman of the Homeland Security Academic Advisory Council’s Subcommittee on Cybersecurity, testified that cybersecurity is “not just a computer field, but one that gives opportunities for individuals who are in a variety of different fields (2014).“

An analysis of the aforementioned 35 Knowledge, Skills and Abilities (KSAs) of Cybersecurity professionals (National Initiative for Cybersecurity Careers and Studies, 2014) indicates that only 37% of the KSAs are related to technology skills: the remainder are related to management, leadership/ organizational dynamics, communications and general business skills (see Appendix A). A recent SANS Analyst Survey (2014) also confirmed that the top items that cybersecurity professionals focus on today—more that 40% of their time—are related to management/ administration and leadership. It also demonstrates that essential cybersecurity job requirements include soft (non-technical) skills, specifically: leadership, communications ability, and interpersonal skills. Thus while higher education may not be able to keep up with rapidly changing technology, it can provide a solid foundation for emerging cybersecurity professionals.

## Balancing Technical and Soft Skills

There is an abundance of cybersecurity degree programs at the graduate level, and these are vital for enhancing the skills of mid-level professionals, often those already working in information technology who desire to specialize in security. About a third of the nation's community colleges also offer degrees in information security and cybersecurity, and they are well-qualified to develop a large number of highly skilled cybersecurity technicians (Homeland Security Academic Advisory Council, 2014).

There is a notable gap at the undergraduate level, which produces most junior or emerging professionals. Frequently, the hiring qualifications for cybersecurity professionals require a bachelor's degree. Federal job standards often preclude applicants with just an associate's degrees from even applying for many entry-level cybersecurity positions

Although not common, particularly at many of the nation's brick & mortar institutions, a bachelor of science in cybersecurity could better prepare qualified students to enter the field of cybersecurity as emerging professionals. A curriculum for such a program would have to strike the balance between providing a technological grounding and developing the required soft skills. This is what American undergraduate education traditionally does best—developing the whole person. More importantly, focusing at the bachelor degree level should enable the graduate to learn how to learn, and help him or her to keep up with rapid changes in the field.

Such a program should empower graduates to be able to:

- Effectively lead efforts to improve its cybersecurity in an organization through collaboration and change management.
- Conduct cybersecurity research and prepare recommendations that can be used to enhance an organization's security standards against threats.

- Apply ethical decision-making models to cybersecurity challenges.
- Monitor information technology (IT) security trends regarding threats and critically assess current information assurance practices and countermeasures.
- Recognize the global threats to cyber networks, and assess the risks associated with an organization's systems.
- Design broad and holistic security solutions, recommend required changes for their organization, and manage the implementation of security systems including policies and procedures.

Despite their importance, such an educational approach would generally not provide the technical certifications valued by and important to public and private employers. Instead it assumes that employers accept that burden. In fact, most employers—approximately 80%--already pay, completely or partially, for the costs of certification for its employees (SANS, 2014). Therefore, given the dynamic changes in technology and the variable needs of organizations, higher education institutions should not try to keep up with it nor provide such training to its students.

## Conclusion

For our nation, adopting such a strategy for obtaining and developing emerging cybersecurity professionals will require a reframing of expectations. It should be recognized that it is unrealistic to expect colleges and universities to produce junior cybersecurity professionals who are completely knowledgeable in all of the current technological tools and ready to instantly respond to a system intrusion. The expectation should be instead that higher education will produce graduates who understand cybersecurity basics, who can see the big picture of how their efforts fit into those of the organization's, who are quick learners committed to lifelong skills development, and are ready to take a leadership role as they begin their journey as cybersecurity professionals.

## REFERENCES

Burning Glass (2016, February 8). A critical skills gap: Demand soars for cybersecurity experts across many industry sectors. *Business West*, p. 8.

Cybersecurity professional trends: A SANS survey. (2014, May). Bethesda, MD: SANS Institute.

Homeland Security Academic Advisory Council. (2014, October 22). Briefing Materials. Retrieved at https://www.dhs.gov/sites/default/files/publications/October%2022_HSAAC_Member_Briefing_Materials.pdf

Lemos, R. (2013, November 19.) Cyber-security training a top priority for industry, government. *eWeek*, 1-1.

Morgan, S. (2016). One Million Cybersecurity Job Openings in 2016. Forbes. Retrieved from http://www.forbes.com/sites/stevemorgan/2016/01/02/onemillion-cybersecurity-job-openings-in-2016/#17a1fb107d27

National Initiative for Cybersecurity Careers and Studies. (2014). Security Program Management (Chief Information Security Officer). Retrieved at http://niccs.us-cert.gov/training/tc/framework/spec-area-detail/30

Perry, W. (2012). Cybersecurity is mission critical. *BizEd*, 11(4), 36-41.

Setalvad, A. (2015). Demand to fill cybersecurity jobs booming, Retrieved at http://peninsulapress.com/2015/03/31/cybersecurity-jobs-growth/

## APPENDIX A. CYBERSECURITY PROFESSIONAL JOB TASK ANALYSIS

According to the National Initiative for Cybersecurity Careers and Studies (2014) there are 35 tasks that a cybersecurity professional performs. The table below analyzes those tasks to categorize their skills domain, listing the primary domain and any secondary domain where it might overlap. The following codes are used:

- **INFO**. Technical skills and knowledge related to Computer Science and/or Information Technology.
- **MGMT**. Common management skills.
- **ORG**. Organizational effectiveness and leadership skills.
- **COM**. Communication skills.

| TASK | PRIMARY SKILL SET | SECONDARY SKILL SET |
|---|---|---|
| Acquire and manage the necessary resources, including leadership support, financial resources, and key security personnel, to support IT security goals and objectives and reduce overall organizational risk | MGMT | ORG |
| Acquire necessary resources, including financial resources, to conduct an effective enterprise continuity of operations program | MGMT | MGMT |
| Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, systems, and elements | MGMT | COM |
| Advise senior management (e.g., CIO) on risk levels and security posture | COM | INFO |
| Collaborate with organizational managers to support organizational objectives | ORG | |
| Collaborate with stakeholders to establish the enterprise continuity of operations program, strategy, and mission assurance | ORG | INFO |
| Communicate the value of IT security throughout all levels of the organization stakeholders | COM | ORG |
| Continuously validate the organization against policies/guidelines/procedures/regulations/laws to ensure compliance | INFO | |
| Define and/or implement policies and procedures to ensure protection of critical infrastructure (as appropriate) | COM | INFO |
| Ensure all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization | INFO | MGMT |

| TASK | PRIMARY SKILL SET | SECONDARY SKILL SET |
|---|---|---|
| Ensure security improvement actions are evaluated, validated, and implemented as required | INFO | |
| Establish overall enterprise information security architecture (EISA) with the organization | INFO | ORG |
| Evaluate cost benefit, economic, and risk analysis in decision making process | MGMT | |
| Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities, and recommend improvements | MGMT | INFO |
| Forecast ongoing service demands and ensure security assumptions are reviewed as necessary | INFO | MGMT |
| Identify alternative information security strategies to address organizational security objective | INFO | |
| Identify IT security program implications of new technologies or technology upgrades | INFO | |
| Interface with external organizations (e.g., public affairs, law enforcement, Command or Component Inspector General) to ensure appropriate and accurate dissemination of incident and other Computer Network Defense information | COM | INFO |
| Interpret and/or approve security requirements relative to the capabilities of new information technologies | INFO | |
| Interpret patterns of non compliance to determine their impact on levels of risk and/or overall effectiveness of the enterprise | MGMT | INFO |
| Lead and align IT security priorities with the security strategy | ORG | INFO |
| Lead and oversee information security budget, staffing, and contracting | MGMT | INFO |
| Manage the monitoring of information security data sources to maintain organizational situational awareness | INFO | |
| Manage the publishing of Computer Network Defense guidance (e.g., TCNOs, Concept of Operations, Net Analyst Reports, NTSM, MTOs, etc.) for the enterprise constituency | MGMT | INFO |
| Manage threat or target analysis of Computer Network Defense information and production of threat information within the enterprise | INFO | |
| Monitor and evaluate the effectiveness of the enterprise's IA security safeguards to ensure they provide the intended level of protection | INFO | |

| TASK | PRIMARY SKILL SET | SECONDARY SKILL SET |
|---|---|---|
| Oversee policy standards and implementation strategies to ensure procedures and guidelines comply with cybersecurity policies | ORG | INFO |
| Oversee the information security training and awareness program | MGMT | |
| Participate in Risk Governance process to provide security risks, mitigations, and input on other technical risk | INFO | |
| Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals | ORG | COM |
| Provide enterprise IA and supply chain risk guidance for development of the Continuity of Operations Plans | INFO | COM |
| Provide leadership and direction to IT personnel by ensuring that IA security awareness, basics, literacy, and training are provided to operations personnel commensurate with their responsibilities | ORG | MGMT |
| Provide technical documents, incident reports, findings from computer examinations, summaries, and other situational awareness information to higher headquarters | COM | |
| Recommend policy and coordinate review and approval | MGMT | INFO |
| Track audit findings and recommendations to ensure appropriate mitigation actions are taken | MGMT | |

| | | | |
|---|---|---|---|
| **INFO** | 13 | 11 | **INFO** |
| **MGMT** | 11 | 4 | **MGMT** |
| **ORG** | 6 | 3 | **ORG** |
| **COM** | 5 | 3 | **COM** |

| | |
|---|---|
| 35 | 21 |