Discovering a Profile for Protect and Defend: Penetration Testing

Morgan A. Zantua[1(✉)], Viatcheslav Popovsky[2], Barbara Endicott-Popovsky[1], and Fred B. Holt[1]

[1] Center for Information Assurance and Cybersecurity, University of Washington, Seattle, WA, USA
{zan5, endicott, fbholt}@uw.edu
[2] University of Idaho, Moscow, ID, USA
dr_popovsky@hotmail.com

Abstract. UW CIAC's inter-collegiate research team has extended the World of Work Inventory (WOWI) to four specific job roles that incorporate penetration testing: Cybersecurity Defense Analyst, Cybersecurity Defense Infrastructure Responder, Cybersecurity Incident Responder, and Vulnerability Assessment Analyst. Identification of these statistically validated profiles can support methodologically based recruitment of high prospective candidates from diverse backgrounds and can inform career guidance protocols for these roles. The WOWI is a statistically validated multi-dimensional career assessment tool. Training data is gathered from a sample of people currently working in the roles, and the instrument identifies profiles for predicting successful candidates across aptitude, personality types, and interests. For this research, we selected the four roles that utilize the task of penetration testing within the category Protect and Defend, in the NIST NICE 800-818 Cybersecurity Workforce Framework. [1] Penetration testing is a skill that is in high demand in career pathways within government, industry and the military.

Keywords: Career guidance · Cybersecurity Workforce Framework Protect and Defenders

1 Background

Projections based on "A Human Capital Crisis in Cybersecurity" [2] in 2010 are being dwarfed by current projections for skilled cybersecurity professionals [3]. Recent projections by Tech Republic and Forbes indicate global projections of 1.8 million to 2.0 million unfilled cybersecurity jobs by 2022 [4, 5]. While IT has been traditionally considered the entry way into cybersecurity positions, the existing IT workforce and current IT-based programs are inadequate to meet the growing demand for workforce and professional development in cybersecurity.

Capacity is not the only challenge. The nature of cybersecurity careers and consequently the curricula for the training programs is shifting as well. As we transition from the Information Age into the Cyber-Mental Age [6] cybersecurity has to be fully

P. Zaphiris and A. Ioannou (Eds.): LCT 2018, LNCS 10925, pp. 530–540, 2018.
https://doi.org/10.1007/978-3-319-91152-6_41

integrated into all aspects of modern day society. Securing the Internet of Things and intelligent machines will require cross-disciplinary skills and knowledge beyond IT skills.

As NICE works to define cybersecurity pathways, UW CIAC has begun developing career guidance tools for use by candidates, counselors, academics, and practitioners. These career guidance tools estimate the multi-disciplinary aptitudes, soft skills, and character considerations, since integrity, trust and productive workplace behavior are important considerations for professionals with access to high value information.

2 Professionalization of Cybersecurity: Career Profiling and Professional Development

Initiatives to professionalize cybersecurity are underway. Research by Dr. Diana Burley of George Washington University proposes cybersecurity workforce development benchmarked against professionalization of the medical profession [7]. Building upon the medical model analogy, the UW CIAC team adapted research methodology building a psychological profile for Surgical Burn Unit residents as a protocol for selecting talent into cybersecurity.

In 2010 a team of psychologists published the "Psychological Profile of Surgeons and Surgical Residents" [8] a research project to ultimately increase retention of surgical residents. The project utilized two of three components of a validated assessment tool and focused on the Psychological Profile component. One scale, Career Aptitude, was not engaged for surgeons and surgical residents given the rigor required to progress through medical school into residency status and beyond. Cybersecurity leaders and employers emphasize the need to identify fundamental qualities that underlie reliability, ethics and trustworthiness to build a strong cyber workforce. Deficiencies in these qualities of character result in 'insider threat' concerns, which are a concern across all sectors. Trade journals and industry publications document the high cost of counterproductive workplace behavior when employees are not screened for honesty, integrity, positive fiscal attitudes and pro-social behavior. [9–11] Integrity First assesses five factors driving an individual's integrity-related behavior in the workplace, which ultimately impacts an organization's ROI [12]. A more detailed description of the dimensions of both tools, WOWI and Integrity First, is provided below.

A literature review of psychological career profiling across the medical field revealed a body of knowledge delineating differences between dermatologists, surgeons, radiologists, internists, family practice etc. [13, 14]. Following this example, we would ultimately like to profile all 35 career pathways within the field of cybersecurity. For the scope of this initial research project, we select two job roles to adapt the methodological approach from a mature profession like medicine to the emerging profession of cybersecurity.

The UW CIAC Research team reviewed the seven career pathways listed in the NIST NICE Cybersecurity Workforce Framework ('Framework') [15].

The interactive tool www.cyberseek.org provides an interactive heat map of supply and demand in 340 markets within the United States. The research team used the heat map for supply and demand, interviews with hiring managers, and consideration of the

knowledge unit (KU) maps, to select the two job roles to study. Penetration testing was selected based upon the high demand for this specific skill set. 2017 witnessed the acceleration of ransom ware and increasing attacks from global cyber actors, escalating individuals with penetration testing skills as the most desired cybersecurity workers [4] (Table 1).

Table 1. NICE Framework workforce categories

Securely Provision (SP)	Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development
Operate and Maintain (OM)	Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security
Oversee and Govern (OV)	Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work
Prated and Defend (PR)	Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks
Analyze (AN)	Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence
Collect and Operate (CO)	Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence
Investigate (IN)	Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, arid digital evidence

For the second job role, we selected careers that emphasized the communication, business, and policy aspects of cybersecurity [4]. Leaders also remain in high demand in cybersecurity, so we selected the category Oversight and Governance as the second career pathway. This part of the research study is the topic of another paper.

To study penetration testing, we selected all four specialty areas under the category Protect and Defend, in the Framework [16]. The Framework does not presently contain a specific job description for penetration tester. It identifies four specialty areas within the Protect and Defend category in which penetration testing is listed as a task: Cybersecurity Defense Analyst (CDA), Cybersecurity Defense Infrastructure Support (INF), Incident Response (CIR) and Vulnerability Assessment and Management (VAM).

Moreover, organizations have not yet fully adopted the Framework. Consequently, penetration testers' actual job descriptions had to be collected and analyzed against the four Protect and Defend job roles to align results across the four work roles within Protect and Defend described in Table 2 [16].

Table 2. .

NICE SPECIALTY Area work role	NICE specialty area definition	Work role definition	Work role ID
CYBERSECURITY DEFENSE ANALYST (CDA) Cyber Defense Analyst	Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network to protect information, information systems, and networks from threats	Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats	PR-CDA-001
CYBERSECURITY DEFENSE INFRASTRUCTURE SUPPORT(INF) Cyber Defense Infrastructure Support Specialist	Tests, implements, deploys, maintains, reviews, and administers the infrastructure hardware and software that are required to effectively manage the computer network defense service provider network and resources. Monitors network to actively remediate unauthorized activities	Tests, implements, deploys, maintains, and administers the infrastructure hardware and software	PR-IN F-001
INCIDENT RESPONSE(CIR) Cyber Defense Incident Responder	Responds to crises or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities	Investigates, analyzes, and responds to cyber incidents within the network environment or enclave	PR-CIR-001

(*continued*)

Table 2. (*continued*)

NICE SPECIALTY Area work role	NICE specialty area definition	Work role definition	Work role ID
VULNERABILITY ASSESSMENT MANAGEMENT (VAM) Vulnerability Assessment Analyst	Conducts assessments of threats and vulnerabilities; determines deviations from acceptable configurations, enterprise or local policy; assesses the level of risk; and develops and/or recommends appropriate mitigation countermeasures in operational and nonoperational situations	Performs assessments of systems and networks within the network environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in- depth architecture against known vulnerabilities	PR-VAM-001

3 Materials and Methods

3.1 Participants and Site Selection

Cybersecurity professionals from an array of Pacific Northwest corporations, state and municipal government, and the Washington Air National Guard 252nd Cyberspace Operations Group are scheduled to complete the assessment instruments in early 2018.

Site selection is based upon multiple factors. Organizational support, manager and subjects' understanding how their contribution impacts the professionalization and quality development of cybersecurity talent are key factors. Criteria selection identified organizations with mature penetration testing functions. Departments with a sufficient number of employees, ideally more than eight, functioning primarily as penetration testers, or working within the four job titles identified by NICE, have been recruited to ensure that normative scaling can be accomplished. Confidentiality of subjects is a requirement in this study

Diversity of organizations provided another selection criteria. Initial outreach to the National Guard provided multi-dimensional aspects. Team members included in the National Guard sites are 'traditional' service members who attend monthly drill week-ends and, in most situations hold civilian positions in a variety of industries. Additional diversity of organization selection includes telecommunications, software development, health care, travel, aerospace, retail and government. On-site proctored data collection of the assessment tool is scheduled during the first quarter of 2018. Statistical analysis of data is scheduled for second quarter 2018 with dissemination of results being prepared and delivered in third quarter 2018.

3.2 Assessment Tools

Two validated on-line instruments were utilized to measure cybersecurity professionals. Assessment tools generally capture aptitude or interest; but rarely are psychological profiles combined in the same instrument. The World of Work Inventory (WOWI) collects data from subjects in all three dimensions. Measuring integrity is the fourth dimension incorporated through the Tescor Survey, also known as Integrity First.

4 The World of Work Inventory

The WOWI provides three subscales measuring career training potential (CTP), Job Satisfaction Indicators (JSI) and Career Interest Activities (CIA). Using a nomothetic approach, CTP assesses verbal, numerical, learning style, spatial ability, mechanical electrical and organizing skills with an added feature of this comparison scale also measures for subject's motivational levels in each of these seven areas. (Table 3) [17].

Table 3. Measurements of Career Training Potential (CTP)

Verbal	Ability to read and comprehend words. Predictor along with the numerical score of ability to do school work
Numerical	Ability to manipulate the language of numbers. Indicates understanding and skill in performing basic mathematical functions
Abstractions	Potential in the area of figuring out problems through a logical procedure. Ability to solve problems by means of size, position, shape or quantity without assistance from words or numbers
Spatial-Form	Ability to visualize and think in three dimensions. Ability to formulate a finished product from seeing the visual plans. Potential to sense forms and positions of things in space
Mechanical/Electrical	Potential to construct, operate and repair machinery and understand physical forces. Also includes the influence of prior knowledge and understanding of electricity, electronics and electromagnetics

The second and third subscales, JSI and CIA utilize ideographic scales. The JSI subscales measure twelve characteristics comprising psychological workstyle preferences (Table 4).

The CIA subscale measures 17 Career Interest Activities corresponding to Table 5:

5 Integrity First

Integrity First is used during recruitment to identify and remove candidates with Counterproductive Workplace Behavior (CWB) from the hiring process. [18] This assessment adds a dimension not covered within career aptitude, psychological and interest assessments. Businesses desire ethical behavior and integrity in their employees; cybersecurity managers, military and civilian, deem ethics, integrity and

Table 4. Characteristics of Job Satisfaction Indicators (JSI) subsets

Versatility	+	Likes variety and change; several things going on at once
	−	Likes to concentrate on 1 task at a time; a linear approach to work
Adaptable to repetitive work	+	Enjoys predictability; activities in a set order
	−	Likes spontaneity; uncomfortable with tasks that repeat in a short time frame
Adaptable to performing under specific instructions	+	Adjusts to being monitored; likes to follow set policies, procedures, recipes, instructions, blueprints, etc.
	−	Likes general direction/instruction; uncomfortable with close supervision
Dominant	+	Likes to lead; be responsible for decisions; is self-directed
	−	Prefers to be in a support role; dislikes being responsible for others
Gregarious isolative	+/+	Likes to work with others, but also likes to be alone to focus on work and get it done
	±	Likes people and does not like being alone; likes being a team player
	∓	Dislikes spontaneous interruption and likes being in control of when others see them
	−/−	Not motivated by a traditional work environment
Influencing	+	Likes to sell products, services or ideas; enjoys persuading, impressing, and motivating others
	−	Likes to be in situations where there is no conflict; is uncomfortable having to persuade, motivate, or sell to others
Self-controlled	+	Likes to work under pressure, deadlines, and in crisis situations; tends to procrastinate
	−	Prefers calm atmosphere; dislikes constantly working under pressure, against tight deadlines, and meeting demanding quotas
Values	+	Likes to make value judgments; has an intuitive approach to making decisions and solving problems
	−	Dislikes making decisions using intuition or hunches
Objective	+	Likes to problem-solve in a rational way; relies on facts and data
	−	Does not like to rely on facts to make decisions
Subjective	+	Enjoys being self expressive; likes to be creative; is uncomfortable conforming to others' standards of style
	−	Does not have a strong drive to be self-expressive or creative
Rigorous	+	Has integrity of workmanship; tendency toward perfectionism; likes to be detail- oriented
	−	No need for exacting results, likes the big picture, the bottom line; dislikes focusing on details

Table 5. .

CIA subscale	Characteristics of career Interest Activities Subscale
Public service	Helping others by providing specialized information and services. Includes occupations in medicine, law, education, religion, library work, counseling, the social sciences, etc.
The sciences	Applying research methods and statistics to solve theoretical and applied problems in the physical, life and social sciences
Engineering and Related	Using the principles of engineering and physics for the design of machines, materials, instruments, structures, processes and services
Business relations	Collecting, analyzing, advising, and making decision based on a variety of data sources. Includes occupations in accounting, insurance, finance, purchasing personnel, human resources, etc.
Managerial	Controlling, directing, and organizing the work of others in a wide range of settings. Requires knowledge of business principles, business operations, and human behavior
The arts	Integrating personal expression and art concepts, techniques, and processes to develop works which elicit an emotional or esthetic response. Includes acting, sculpting, painting, etc.
Clerical	Compiling, recording, communicating, computing, copying, and otherwise organizing information for others
Sales	Interacting with and influencing others in favor of certain products, services, or ideas
Service	Helping individuals with their personal wants and needs. Includes occupations in cosmetology, day care, recreation, hospitality, food-and-beverage preparation and service, etc.
Processing Machine Work Bench Work Structural Work Mechanical Work Graphic Arts Mining	Working with tools, equipment, materials, products, structures, structural parts, or operating machinery. Includes mechanical, electrical, masonry, and tool and die work, carpentry, plumbing, mining, drafting, factory work, etc.

positive workforce behavior essential when assembling cybersecurity pen testing teams. CWB falls into four fundamental categories: employee theft, hostility, drug abuse and hostility. Using overt testing methods, candidates chose one of four answers to direct questions regarding attitudes and high risk workplace behavior [19]. A more comprehensive list of CWB is provided in Table 6 [20]. The UW CIAC research team acknowledged there is a gap in career instruments including the WOWI, to overtly measure characteristics of integrity and ethics.

Table 6. Examples of counterproductive workplace behavior

1. Workplace Violence
2. Alcohol and illicit drug abuse
3. Theft – Cash, Merchandise
4. Theft – IP data, trade secrets, client list
5. Theft – Faking time cards, record keeping
6. Theft – Faking injury, sickness
7. Identity Theft
8. Theft – Unauthorized Discounts
9. Bullying – physical, verbal
10. Disrespecting – management, fellow employees
11. Disrespecting customers, vendors
12. Low regard for quality service, products
13. Low regard for company reputation
14. Low regard for following company rules
15. Create & circulate miscommunication, untrue rumors
16. Willful destruction of company property

6 Conclusion

6.1 Participants and Site Selection Revisited

Organizational culture impacts data collection. Washington's Air National Guard, government agencies and universities conduct annual performance reviews; but not all of these organizations rank and stack employee perfor. Military organizations have ingrained merit and ranking systems and conduct structured performance reviews. Government and academic organizations, while annual reviews are conducted, no merit ranking system is utilized.

Corporations in the Pacific Northwest, for the most part, migrated from strict adherence to a military merit rating system in favor of talent development and performance appraisals [20] based upon on-going adaptation of Douglas McGregor's Theory X and Y

[21] Employees are assessed from multiple perspectives, personal and team interaction and contributions to corporate success are acknowledged, in some corporations, by bonuses [22]. This metric may supplant managerial ranking. Managerial ranking is being reviewed and compared to a revised Performance Appraisal system identifying end-of-year bonuses as a performance metric.

6.2 Hypothesis

Talent identification in cybersecurity informs the hypothesis that there are statistically significant profiles across measures of aptitude, personality type indicators, interests, and integrity such that (a) these profiles are a reliable predictor of success in careers

within the Protect and Defend category in the NICE Workforce Framework and (b) the measuring instruments for these profiles are robust against biased inputs.

Initial research results focus on CTP, JSI, CIA and results from CWB defining profiles of high performing Protect and Defenders with an emphasis on the four job titles encompassing penetration testing proclivities. Additional research targeting specific job roles in Oversight and Governance, planned for later in 2018, provides the opportunity to compare profile results. Based upon the findings, additional research may be warranted.

References

1. Newhouse, W., Keith, S., Scribner, B., Witte, G.: National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (2017). https://doi.org/10.6028/NIST.SP.800-181
2. Evans, K., Reeder, F.: Human Capital Crisis in Cybersecurity: Technical Proficiency Matters, Center for Strategic Initiatives (2010)
3. Suciu, P.: Tech: Cyber security's ever-growing brain drain. Fortune (2015). http://fortune.com/2015/09/09/cybersecuritys-ever-growing-brain-drain/
4. DeNisco-Rayome, A.: The 3 most in-demand cybersecurity jobs of 2017. TechRepublic. (2017). https://www.techrepublic.com/article/the-3-most-in-demand cybersecurity - jobs-of-2017
5. Kauflin, J.: Forbes. The Fast-Growing Job With A Huge Skills Gap: Cyber Security (2017). https://www.forbes.com/sites/jeffkauflin/2017/03/16/the-fast-growing-job-with-a-huge-skills-gap-cyber-security/#716cca2a5163
6. Gordon, E.E.: Praeger Future Jobs: Solving the Employment and Skills Crisis (2013). ISBN-13:978-1440829338
7. Hoffman, L., Burley, D.L., Toregas, C.: Holistically building the cybersecurity workforce. Commun. IEEE Secur. Priv. **10**(2), 33–39 (2011)
8. Foster, K.N., Neidert, G.P.M., Brubaker-Rimmer, R., Artalejo, D., Caruso, D.M.: Psychological profile of surgeons and surgical residents. APDS Spring Meeting (2010). http://www.wowi.com/about/Psych_Profile_of_Surgeons_and_Surgical_Residents.pdf
9. Durbin, S.: Recode. Insiders are today's biggest security threat (2016). https://www.recode.net/2016/5/24/11756584/cyber-attack-data-breach-insider-threat-steve-durbin
10. Beek, C., McFarland, C., Samani, R.: McAffe Health Warnings, Cyberattacks are targeting the health care industry (2016). https://www.mcafee.com/us/resources/reports/rp-health-warning.pdf
11. Tuutti, C.: Nextgov: The Insider Threat: A Historical Perspective (2016). http://www.nextgov.com/cybersecurity/2016/09/insider-threat-historical-perspective/131613
12. Sturman, M.C., Sherwyn, D.J.: The Utility of Integrity "Testing for Controlling Workers' Compensation Costs", Cornell University, Cornell Hospitality Quarterly, 2009, November [13.14] [15 – Workforce framework] (2009)
13. Maron, B.A., Fein, S., Maron, B.J., Hillel, A.T., El Bagdadi, N.M.: Ability of prospective assessment of personality profiles to predict the practice specialty of medical student. Proc. (Bayl. Univ. Med. Cent.). **20**(1), 22–26 (2007)
14. Borges, N., Savickas, M.L.: Personality and medical specialty choices: a Literature review and integration. Career Assess **10**, 362–380 (2002)

15. Newhouse, W., Keith, S., Scribner, B., Witte, G.: National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, pp. 11–32 (2017). https://doi.org/10.6028/NIST.SP.800-181
16. Newhouse, W., Keith, S., Scribner, B., Witte, G.: National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (2017). https://doi.org/10.6028/NIST.SP.800-181. Reference Spreadsheet for NIST Special Publication 800-181 https://www.nist.gov/file/372581
17. Neidert, G.P.M.N., Ortman, N.I.: Interpretation Manual for the World of Work Inventory, 5th edn. World of Work Inc., Tempe (2001)
18. Johnson, R.: Integrity Testing: Why and How to Implement Integrity Testing as an Important Part of your Talent Management Cycle. Merchants Informations Solutions, Inc. (2013)
19. Cullen, M.J., Sackett, P.R.: Personality and Counterproductive Workplace Behavior, Chap 6 150–160 Personality and Work Reconsidering the Role of Personality in Organizations 440 p. (2004)
20. Cappelli, P., Tavis, A.: The Performance Management Revolution. Harvard Business Review, October 2016
21. Kopel, R.D., Prottas, D.J., Davis, A.L.: Douglas McGregor's theory X and Y: toward a construct-valid measure. J. Managerial Issues **20**(2), 255–271 (2008). http://www.jstor.org/stable/40604607
22. Hearn, S.: Ditch Annual Appraisals: Continuous Performance Management is the Way Forward. Entrepreneur (2017). https://www.entrepreneur.com/article/290900