Toward Cyber Workforce Development: An Exploratory Survey of Information Security Professionals

Steven Wu and David Schuster

San José State University

Introduction

- There is a shortage of cybersecurity professionals, those who "protect, monitor, analyze, detect and respond to unauthorized activity" ("Computer Network Defense," 2015, para. 1).
- With this exploratory research, we provide the foundation to train future cybersecurity professionals by eliciting knowledge from professionals (subject matter experts, SMEs) currently working in the field.
- We focused on several challenges encountered in cyber work, including skill development, threat response, and team organization.

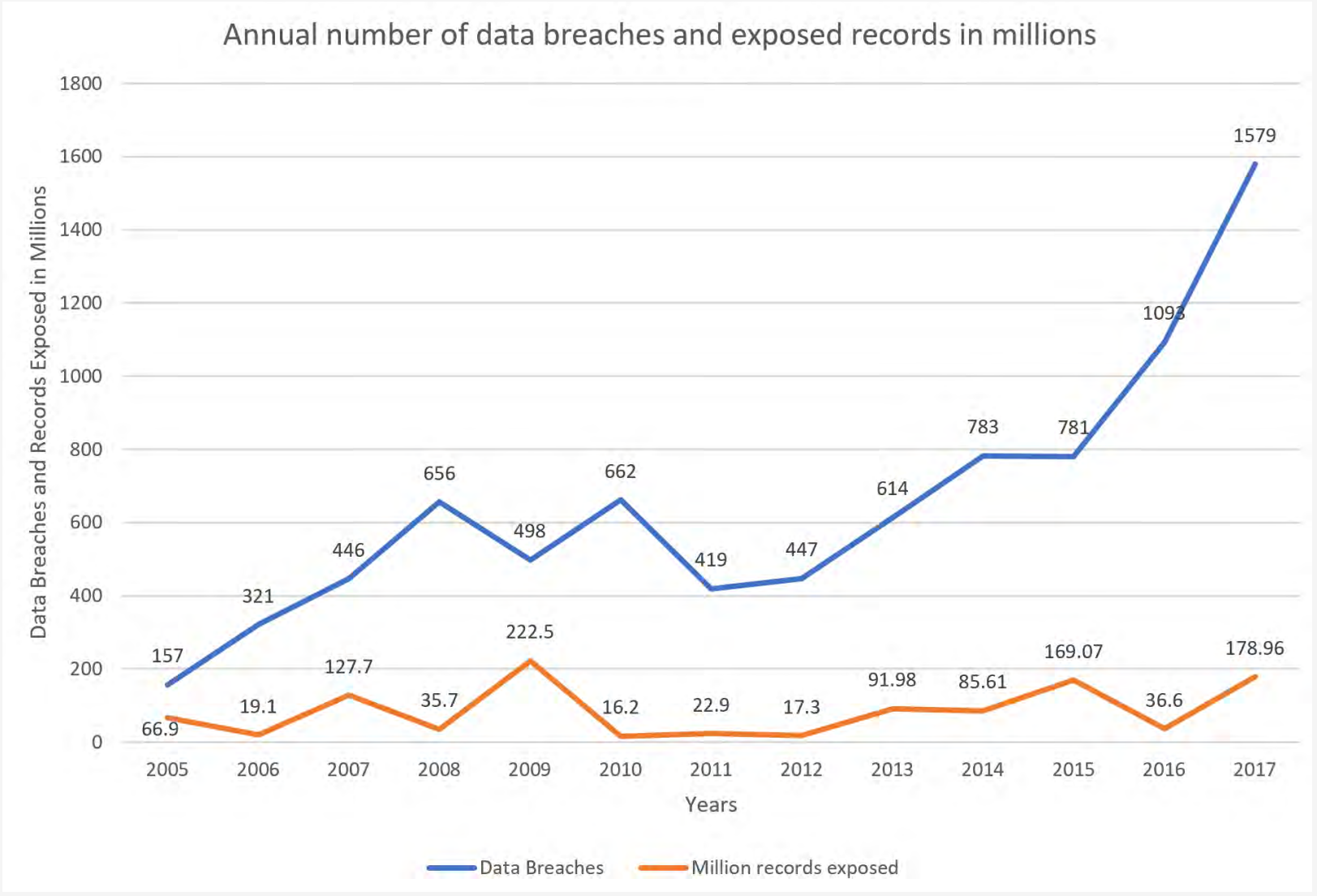


Figure 1. Graph showing rise in data breaches in the United States (Identity Theft Resource Center; CyberScout, 2018).

SME Knowledge Elicitation, Company 1: Method

5 SME Participants (4 male, 1 female)

- Roles such as information security investigator, information security engineer, and management

Elicitation Survey

- Qualitative and Quantitative questions
- Questions addressed Skill Development, Threat Response, Team Organization, and Major Challenges

SME Knowledge Elicitation, Company 2: Method

6 SME Participants (all male)

- Roles such as information security engineer, information security architect, and director of information security

Elicitation Survey

- Expanded upon the survey used at Company 1
- Questions on skill development and threat response expanded to allow more depth in answers
- Included section to evaluate alignment with National Initiative for Cybersecurity Education (NICE) framework

Results

Skill Development

- High variability in career training paths
- Wide variety in levels of education and certifications among cybersecurity professionals, even within the same job role
- SMEs said that certifications were useful, but were not necessarily indicative of one's capability
- Not necessarily one career path to being a cybersecurity professional

Threat Response

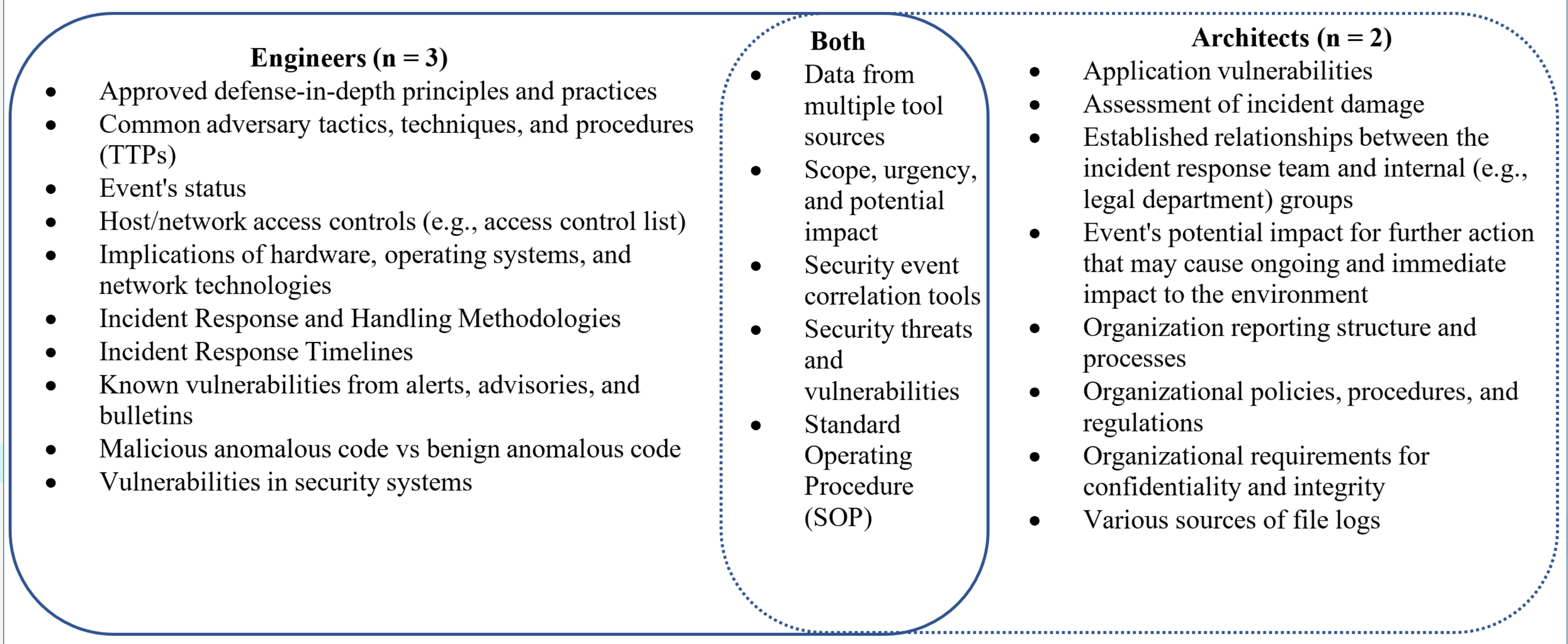
- Variability in usage of threat severity taxonomy
- No observed standardized system of categorization for threat severity
- All SMEs categorized high and low levels of threat, but segmentation between high and low varied.

Team Organization

- Teams working remotely across the globe are common

Major Challenges

- Signal detection is difficult in cybersecurity:
  Target signals are uncommon and of high importance while volume of noise is high
- Being heard within organizations can be difficult
- Translating best practices into implementation



Engineers (n = 3)

- Approved defense-in-depth principles and practices
- Common adversary tactics, techniques, and procedures (TTPs)
- Event's status
- Host/network access controls (e.g., access control list)
- Implications of hardware, operating systems, and network technologies
- Incident Response and Handling Methodologies
- Incident Response Timelines
- Known vulnerabilities from alerts, advisories, and bulletins
- Malicious anomalous code vs benign anomalous code
- Vulnerabilities in security systems

Both

- Data from multiple tool sources
- Scope, urgency, and potential impact
- Security event correlation tools
- Security threats and vulnerabilities
- Standard Operating Procedure (SOP)

Architects (n = 2)

- Application vulnerabilities
- Assessment of incident damage
- Established relationships between the incident response team and internal (e.g., legal department) groups
- Event's potential impact for further action that may cause ongoing and immediate impact to the environment
- Organization reporting structure and processes
- Organizational policies, procedures, and regulations
- Organizational requirements for confidentiality and integrity
- Various sources of file logs

Figure 2. NICE Framework concepts with highest importance ratings based on participant job title.

Table 1
Certifications Held by Participants at Company 1

Certification Held	Frequency
CCNA	1
CISSP	1
GSEC	2
SJSU Certificate in Secure Software Engineering	1
Splunk Admin	1

Table 2
Certifications Held by Participants at Company 2

Certification Held	Frequency
CISA	4
CISSP	3
GCIH	3
Others	9

Conclusions

- Confirmed the need for empirically-derived educational pathways for cybersecurity careers to address the workforce shortage. Formalizing the process and skills required for a cybersecurity career are important.
- Remote team members across the globe are common, and could indicate the need to study cybersecurity teamwork.
- Key concepts from NICE framework aligned closely with SMEs
- More work is needed to align certifications, job roles, and industry needs
- Understanding how proficiency in cybersecurity roles is developed can inform training in these new cybersecurity workers.

Our Future Directions and Current Work

- Apply qualitative methods to examine development of proficiency in cybersecurity professionals
- Develop a training paradigm to efficiently train novice cybersecurity professionals

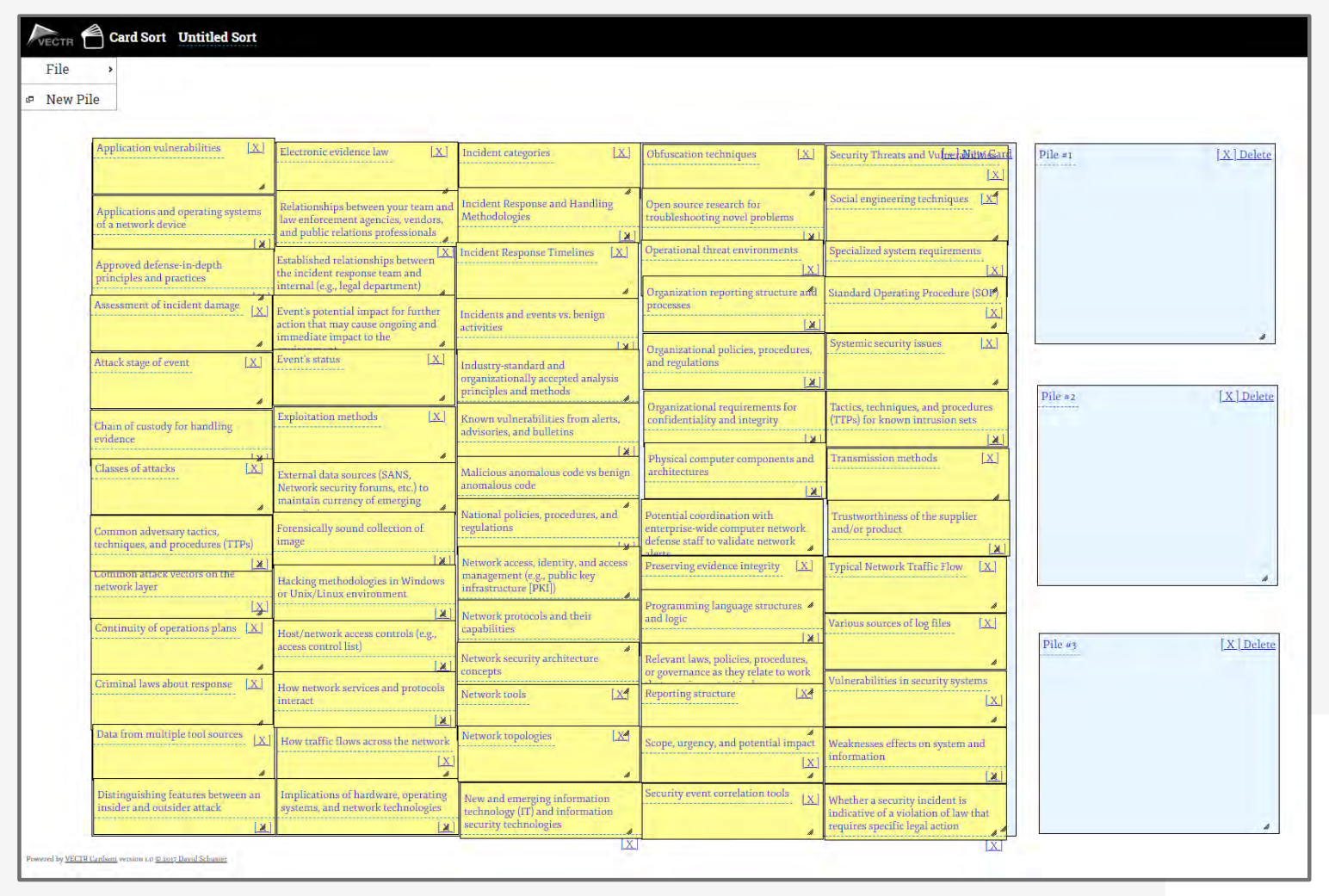


Figure 3. Sample of Card Sort used to elicit knowledge

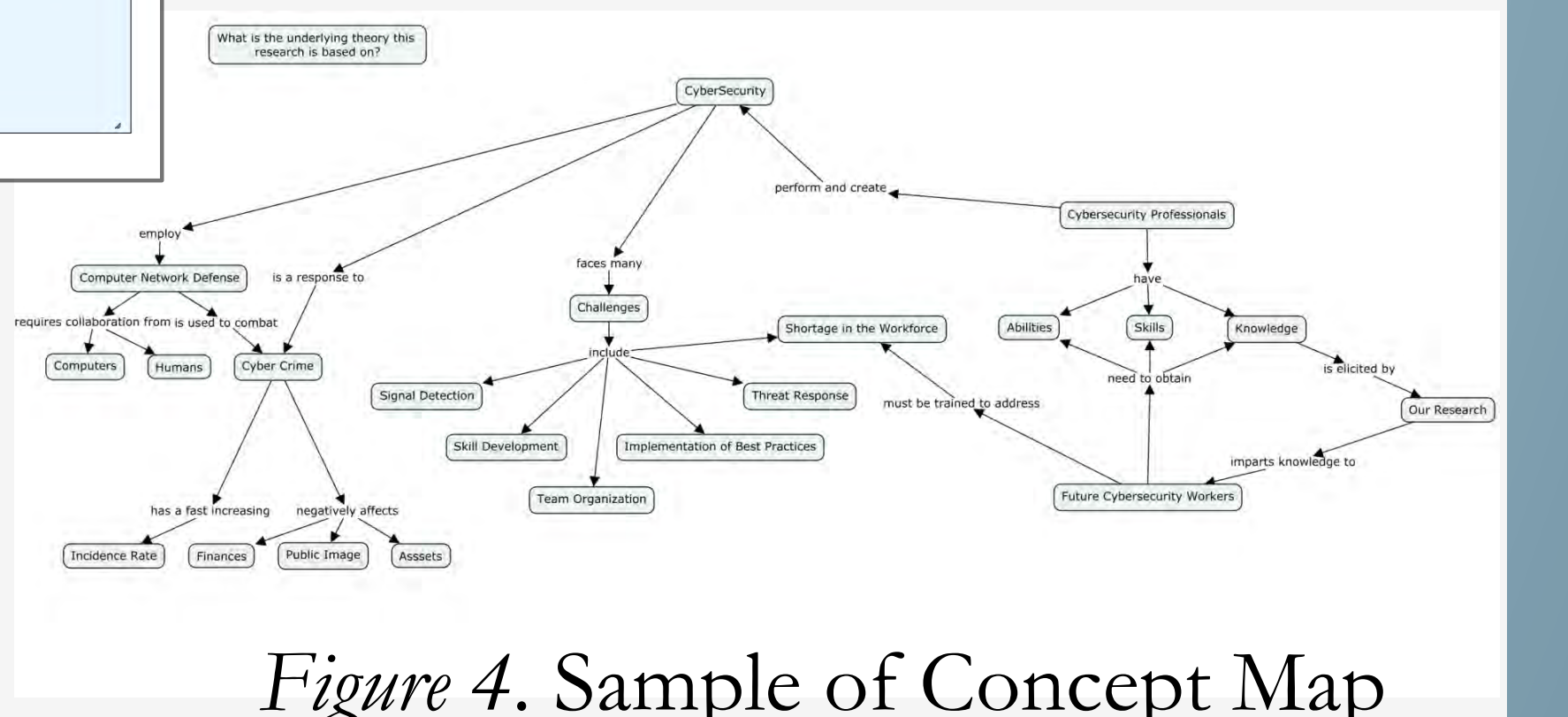


Figure 4. Sample of Concept Map used to elicit qualitative data

References and Acknowledgements

Computer Network Defense [Web page]. (2015). Retrieved from http://www.dtic.mil/doctrine/dod_dictionary/data/c/10869.html

Identity Theft Resource Center; CyberScout. (2018). Annual number of data breaches and exposed records in the United States from 2005 to 2018 (in millions). In Statista – The Statistics Portal. Retrieved September 19, 2018, from https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

This work is based upon work supported by the National Science Foundation under Grant No. 1553018. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.