Expert Assessment of the Top Platform Independent Cybersecurity Skills for Non-IT Professionals

Melissa Carlton, Yair Levy
Graduate School of Computer and Information Sciences
Nova Southeastern University
Ft. Lauderdale, FL, USA
Email: {mc2418, levyy}@nova.edu

Abstract—Cybersecurity threats are causing substantial financial losses for individuals, organizations, and governments. Information technology (IT) users’ mistakes, due to poor cybersecurity skills, represent about 72% to 95% of cybersecurity threats to organizations. As opposed to IT professionals, computer end-users are one of the weakest links in the cybersecurity chain, due to their limited cybersecurity skills. Skills are defined as the combination of knowledge, experience, and ability to do something well. Cybersecurity skills are the skills one possesses to prevent damage to IT via the Internet. However, the current measures of end-user cybersecurity skills are based on self-reported surveys. This study is the first phase of a larger research project that is aimed to develop a scenario-based iPad application to measure cybersecurity skills based on actual scenarios with hands-on tasks that the participants complete in demonstrating their skills. To design a measure that has both high validity and reliability, the first phase of the study was set forth to follow the Delphi method in seeking subject matter experts’ opinion on the top platform independent cybersecurity skills for non-IT professionals. A total of 18 experts from the Florida chapter of the InfraGard, a public-private partnership between the United States Federal Bureau of Investigation (FBI)’s cyber division and private sector that focuses on cybersecurity, along with subject matter experts from other federal agencies such as the United States Secret Services’ (USSS) Electronic Crimes Task Force team and industry, took part in our Delphi expert panel process. The exploratory expert panel data was recorded and categorized into similar groups of comments for improvements, along with quantitative rankings. Comments were then solicited again for expert consensus, to derive the rankings of the top nine platform independent cybersecurity skills. The paper ends with some discussion on the next phase of this ongoing research along with some initial implications of the findings to practice and research.

Keywords—cybersecurity; cybersecurity skills; risk mitigation tool; information security skills of non-IT professional; InfraGard-United States Federal Bureau of Investigation expert panel

I. INTRODUCTION

One of the main challenges in the study of information technology (IT) skills is the fact that IT skills have been measured, predominantly in research, based on self-reported survey instruments [1, 2]. Cybersecurity threats and vulnerabilities are causing substantial financial losses for individuals, organizations, and governments all over the world [3, 4]. Cyberwar is another major concern that nations around the world are struggling to get ready to fight or maintain strong defense tactics. It has been found that non-IT computer users’ mistakes, due to poor cybersecurity skills, represent about 72% to 95% of cybersecurity threats and vulnerabilities to organizations [5, 6]. The U.S. National Security Council has developed ‘The Comprehensive National Cybersecurity Initiative’ (CNCI) and one of its main initiatives is to:

Initiative #8. Expand cyber education. While billions of dollars are being spent on new technologies to secure the U.S. Government in cyberspace, it is the people with the right knowledge, skills, and abilities to implement those technologies who will determine success. However, there are not enough cybersecurity experts within the Federal Government or private sector to implement the CNCI, nor is there an adequately established Federal cybersecurity career field. Existing cybersecurity training and personnel development programs, while good, are limited in focus and lack unity of effort. In order to effectively ensure our continued technical advantage and future cybersecurity, we must develop a technologically-skilled and cyber-savvy workforce and an effective pipeline of future employees. It will take a national strategy, similar to the effort to upgrade science and mathematics education in the 1950’s, to meet this challenge. [7]

Yet, the existing measures of cybersecurity skills are dated and limited. Additional work is needed to develop a measure based on scenarios that emulate real-life cases of cybersecurity attacks. Moreover, with the shift from desktop to laptop computers, and in the past decade to mobile devices, there is a need to ensure such measures are not tied to a specific platform and/or operating system. As such, the key objective of this study was to develop a list of the top platform independent skills that will form the basis for the set of scenarios that will capture potential cybersecurity threats. With the massive move into mobile computing and the seamless move between devices that the majority of current employees are engaged in, a critical need emerged to ensure that prior to uncovering the list of the skills, a set of platform independent threats is identified. Once the set of top platform independent threats is identified, a list of matching skills for non-IT professionals can be developed that can form the foundation for the development of the specific scenarios. For example, the threat of malware via e-mail attachment can be assessed via an activity within an e-mail...
attack scenario that provides participants with a list of e-mails in an inbox asking them to identify potentially harmful messages and measure how many of these they identify. Another example of an activity within the e-mail attack scenario is to present participants with two e-mail messages sent from a bank, asking them to identify the one that is a hoax and the one that is real, while asking them to identify all the indicators that triggered the suspicion of the hoax e-mail.

As such, the main goal of this extensive cybersecurity skills research is to develop a prototype Cybersecurity Skills Index (CSI) iPad app. However, before the development of real-life scenarios can be made, our foundational work documented in this paper will outline the process of identifying and validating the specific cybersecurity threats, their matching skills from non-IT professionals, and their ranking (weights) in construction of such novel index. Therefore, the central aim of this phase of our developmental research was to address the following three specific research questions (RQs):

RQ1: What are the top most critical cybersecurity threats that non-IT professionals pose to organizations?
RQ2: What are the matching top cybersecurity skills that non-IT professionals must have to mitigate the top nine most critical cybersecurity threats posed to organizations?
RQ3: What are the weights of the skills that enable a validated aggregation to a benchmarking index of cybersecurity skills?

Given the documented increase in importance of cybersecurity in everyday activity, the significance of this study is substantial. With the limitations that currently exist in the measurement of cybersecurity skills within the research body of knowledge, the development of a scenario-based tool to measure such skills using scores on simulated activities rather than self-reported survey, will help several stakeholders. Ideally, the use of the CSI iPad app will allow organizations to map their human threat-vectors when it comes to employees and the employees of external contractors. A second example includes organizations that use the CSI iPad app to identify groups of employees where additional training in the area of cybersecurity attack prevention should be targeted. The third example includes government recruiters, in conjunction with high school teachers/administrators, which can use the CSI iPad app to identify individuals who demonstrate a high level of cybersecurity skills and may be the appropriate feeders for advanced cyber warrior programs. As seen in the literature review, organizations have an ongoing need for non-IT cybersecurity skilled professionals. Therefore, the arguments discussed later focus mainly on the non-IT professionals representing the corporate organizations.

II. LITERATURE REVIEW

A. Cybersecurity Threats

According to IBM Global Technology Services [6], ‘human error’ was identified as a contributing factor in over 95 percent of all security incidents investigated. Furthermore, opening an infected attachment or selecting an unsafe Universal Resource Locator (URL) was the most prevalent contributing ‘human error’ when it comes to inflicting malware on computing systems [6]. From 2005 to 2012, Privacy Rights Clearinghouse [8] reported over 607 million records lost from nearly 3,500 data breaches. According to Boritz and No [9], in the past government agencies were only involved in egregious privacy breaches. Over a year later, President Barack Obama signed Executive Order No. 13,681 requiring “the use of multiple factors of authentication and an effective identity proofing process” [10] when a U.S. citizen’s personal data is made available through digital applications. Nearly 1.6 billion records were reported lost from 453 data breaches during the period of January 2013 to December 2014 and an additional 454 breaches occurred with an unknown number of lost records [8].

Prior research identified the need for research to address the threats to organizational IT due to vulnerabilities and breaches caused by employees [11, 12, 13]. More than any other internal process or technology, breaches were discovered by end-users armed with the skills needed to quickly identify and report possible cyber espionage occurrences [14]. Technology alone cannot guarantee security. A security risk is often accepted by an end-user when the countermeasure interferes with work productivity [11]. Therefore, the human factor cannot be ignored in corporate security without peril [15]. Most security incidents were attributed to everyday insiders like current or former employees [16]. According to Verizon Communication’s chief security officer, insider threats may be from “a good employee doing righteous work in an insecure manner” [16]. Moreover, it was noted that “unfortunately, even the best security mechanisms can be bypassed through social engineering” [17], which “is now considered the great security threat to people and organizations” [18]. Even amid those who classified themselves as being aware of social engineering techniques, Kvedar, Nettis, and Fulton [19]’s findings suggested an implemented social engineering plot could succeed. An end-user with technology knowledge does not automatically become skilled in cybersecurity [11]. In the work of Qin and Burgoon [20], users had an 18% accuracy in detecting deception. According to Enterprise Risk Management (ERM) [21], not protecting an organization’s information puts “the reputation, success, and survival of the organization at risk.” An example of this occurred in November 2014 when Sony Pictures suffered a data breach that shut down all email communications and computer usage due to a hacker posting threatening messages on company owned computers and obtaining unsecured data files [8]. However, the skills needed to mitigate such cybersecurity threats and to protect corporate IT systems from such data breach attacks can be the difference between experiencing a breach or not.

Thus, the importance of a measure to assess the level of cybersecurity skills held by a non-IT professional is significant.

B. Skills

According to Boyatzis and Kolb [22], as well as Levy [1], skill is a combination of knowledge, experience, and ability that enables end-users to perform well. The acquisition of a skill is a learning process and generally adopts three incremental stages [23, 24]. These stages begin with the initial
acquisition of a skill known as declarative knowledge (Stage 1). During Stage 1, instruction and information about a skill are given to the end-user [23, 25]. Moreover, Stage 1 allows the end-user to establish the knowledge needed as a foundation for later learning stages [24]. The second stage of skill acquisition (Stage 2) allows the learner to practice declarative knowledge and convert it to procedural knowledge [25, 26]. Knowledge becomes better organized and end-users start to connect the actions needed to complete an activity [24]. Next, at the third stage, comes automaticity [25, 27]. End-users progress beyond the initial acquisition stage into an efficient and autonomous stage (Stage 3) by increasing their experience level [23, 28]. Experience positively influences an end-user’s computer usage, which helps establish the needed experience of the skill [24]. The ability to generalize procedures and increase performance occurs during the acquisition of knowledge phases [27]. Over time, Eschenbrenner and Nah [29] identified that skills are honed and competencies are acquired. The skill development stages are shown in Fig. 1.

C. Cybersecurity Skills

Cybersecurity is “the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation” [30]. Cybersecurity also includes the restoration of digital information and communications [31]. Protection of data and information remains in the most vulnerable spot [32]. Humans, despite their intellect, are the most severe threat to an individual’s security [33]. Information is valuable and knowledge protects information from progressively sophisticated cybersecurity threats [33]. Therefore, cybersecurity skills correspond to an individual’s technical knowledge, ability, and experience surrounding the hardware and software required to execute information security in protecting their IT against damage, unauthorized use, modification, and/or exploitation [11]. Cybersecurity is not a solitary occupational category and knowledge, skills, and abilities are needed for more than cybersecurity work [34]. Limited cybersecurity skills contribute to the behavior of users that causes human errors, often unintentional [35]. Likewise, a technology savvy user does not automatically make a cybersecurity savvy user [11]. Thus, it appears that a non-IT professional with limited cybersecurity skills presents opportunities for organizational information vulnerabilities and threats [36].

D. Competence vs. Skills

Bronsburg [37], as well as Morcke, Dornan, and Eika [38] demonstrated the importance of the high-level of skills experienced in the medical and health profession academic programs. The need to include competencies, skills, knowledge, and abilities in the classroom so students had the tools (experience) necessary for future employment were the focus of Havelka and Merhout [39], as well as Rubin and Dierdorff [40]. Havelka and Merhout [39] found that knowledge is obtained through coursework. Whereas, Rubin and Dierdorff [40] found the courses offered by colleges and universities are relevant to the competency level of a student. It was discovered that the maturing of an individual’s knowledge improves skills, which then develops user competency [29]. Moreover, it was previously noted in literature that knowledge gathered by users and honed skills in a certain functional area developed competencies [41]. A misalignment between course offerings and required corporate competencies reduces the individual’s exposure to important knowledge needed to do a task well [40]. Additionally, it was noted that a reasonable degree of competency at a skill “requires at least 100 hours of learning and practice” [23]. An individual’s competency level of a particular skill is valuable; it may influence or even determine an individual’s level of professional success and satisfaction [39]. A user’s computer competence is vital for an organization that relies on its employees to possess skills, (i.e., knowledge, experiences, & abilities) to complete technical tasks [42]. Thus, it appears that competency is acquired after a skill is practiced over time.

III. METHODOLOGY

When judgmental information is essential, prior research has employed the Delphi technique [43, 44]. Using the Delphi technique provides a way and method for consensus-building without direct confrontation among the experts [45]. Characterized as an iterative group communication process, the Delphi technique allows for experts to address complex problems in an effective manner [43, 44, 46]. Prior research, e.g. [47, 48], utilized the Delphi technique for forecasting, issue identification, and concept/framework development. In addition, the Delphi method ensures both reliability and validity as it exposes the study to a panel of differing, and often contradictory, opinions while seeking convergence through subject matter experts’ (SMEs) feedback [48]. This study employed the Delphi technique for the purpose of identifying the indispensable expert opinion of cybersecurity threats and related skills. Key features that are regarded as the Delphi technique include secrecy, iteration, controlled feedback, and statistically clustering the responses [49]. Secrecy was maintained in this study with the use of Web-based questionnaires. Between each questionnaire, feedback was controlled by incorporating the SMEs’ responses into the next questionnaire.

Round one consisted of 12 platform independent cybersecurity threats that were identified after a survey of existing body of knowledge and were presented to SMEs from the Florida chapter of the InfraGard, a public-private partnership between the United States Federal Bureau of Investigation (FBI)’s cyber division and private sector that
focus on cybersecurity, along with subject matter experts from other federal agencies such as the United States Secret Services’ (USSS) Electronic Crimes Task Force team and industry. The SMEs were asked to rank in order of importance the threats that non-IT professionals poses for organizational cybersecurity posture. Based on the SMEs’ feedback, the list of 12 platform independent cybersecurity threats were narrowed to 10 platform independent cybersecurity threats. In the second Delphi technique round, the 10 cybersecurity threats identified as the most significant were then presented to the panel of SMEs in a Web-based survey using a seven-point Likert scale. Based on a score of 1 for strongly disagree and 7 for strongly agree, each of the proposed cybersecurity threats were evaluated to determine 1) if it was valid to be included in the core fundamental cybersecurity threat set; 2) if a proposed platform independent skill is valid or not; and 3) if each proposed skill is independent from other proposed cybersecurity skills. Moreover, the SME panel were asked to provide a ranking of 1, representing the highest threat, to 10, representing a lessor threat. The skill importance weight for each skill was calculated so the lesser threat received a weight closer to 0.0, while the highest ranked threat received a weight closer to 1.0. The threats are based on their skill importance weight in causing harm to organizations and individuals, while forming the foundations for the development of a hierarchical-based indexing to measure an overall measure of cybersecurity skills (i.e. the CSI) in follow-up research.

IV. DATA ANALYSIS AND RESULTS

As seen in the works of Helmer [50], as well as Linstone and Turoff [46], a consensus of SMEs’ opinion emerged with the top nine cybersecurity skills needed for non-IT professionals. Three distinct categories were identified among the cybersecurity threats and identified matching skills: (A) malware; (B) personally identifiable information (PII); and (C) work information systems (WIS) related threats. At the end of the second Delphi round, the difference between the lowest ranked cybersecurity threat/skill and the highest was nearly 2.28. Cybersecurity threat and corresponding skill number 10, preventing unauthorized information system access via workstation lock or log out, was identified as an outlier and the SMEs’ highly recommended discarding it from the list. Table 1 displays the collective results of both Delphi rounds identifying the top nine platform independent cybersecurity skills, their respective category, SME rankings, number of SME responses, ranked weighted total, ranked average, and skill importance weight.

V. CONCLUSION AND DISCUSSION

The main goal of this research study was to develop a list of top platform independent skills that will form the basis for the set of scenarios that will capture potential cybersecurity threats through hands-on tasks. Using the Delphi technique, the top nine most critical threats and related cybersecurity skills were identified by consensus of 18 cybersecurity professionals. The Delphi technique is a popular research tool for identifying and ranking issues within the IT field [43, 44]. To ensure the most reliable and valid results, this study warranted 1) the panel of SMEs remained stable; 2) the amount of time between questionnaires was minimized; 3) clear-cut questions were presented; and 4) consensus was reached with justified feedback [51]. Weighted totals were based on the number of SME responses multiplied times the score for each assigned ranking. This was then divided by the total number of SME responses for determining the final rank of one through nine. Each skill importance weight was based on the individual skill weighted average divided by the total weighted average. These results provide a foundation in achieving the larger research study objectives.

VI. FUTURE RESEARCH

This study was the first phase of a larger research study. The second objective of the larger research study will involve the design and development of scenario-based, hands-on tasks related to each of the nine SME identified cybersecurity skills. In round three of the Delphi technique, SMEs will be asked for feedback regarding the scenario-based, hands-on tasks, and the relationship to the respective skill. At the conclusion of round three, SMEs’ responses will be incorporated into the development of the MyCyberSkills™ iPad app.

While developing and validating such a comprehensive set of scenario-based, hands-on benchmarking index is a good step in the right direction, the process of implementing it in order to actually measure such skills can be challenging. In order to overcome this issue, the third objective of the larger research study was to develop a list of top platform independent skills that will form the basis for the set of scenarios that will capture potential cybersecurity threats through hands-on tasks. Using the Delphi technique, the top nine most critical threats and related cybersecurity skills were identified by consensus of 18 cybersecurity professionals. The Delphi technique is a popular research tool for identifying and ranking issues within the IT field [43, 44]. To ensure the most reliable and valid results, this study warranted 1) the panel of SMEs remained stable; 2) the amount of time between questionnaires was minimized; 3) clear-cut questions were presented; and 4) consensus was reached with justified feedback [51]. Weighted totals were based on the number of SME responses multiplied times the score for each assigned ranking. This was then divided by the total number of SME responses for determining the final rank of one through nine. Each skill importance weight was based on the individual skill weighted average divided by the total weighted average. These results provide a foundation in achieving the larger research study objectives.

<table>
<thead>
<tr>
<th>TABLE I. RANKINGS OF THE TOP NINE CYBERSECURITY SKILLS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Skills</strong></td>
</tr>
<tr>
<td>-------------</td>
</tr>
<tr>
<td>CSS1 - Preventing the leaking of confidential digital information to unauthorized individuals</td>
</tr>
<tr>
<td>CSS2 - Preventing malware via non-secure Websites</td>
</tr>
<tr>
<td>CSS3 - Preventing personally identifiable information (PII) theft via access to non-secure networks</td>
</tr>
<tr>
<td>CSS4 - Preventing PII theft via e-mail phishing</td>
</tr>
<tr>
<td>CSS5 - Preventing malware via e-mail</td>
</tr>
<tr>
<td>CSS6 - Preventing credit card information theft by purchasing from non-secure Websites</td>
</tr>
<tr>
<td>CSS7 - Preventing information system compromise via USB or storage device exploitations</td>
</tr>
<tr>
<td>CSS8 - Preventing unauthorized information system access via password exploitations</td>
</tr>
<tr>
<td>CSS9 - Preventing PII theft via social networks</td>
</tr>
</tbody>
</table>

Totals -> | 941 | 52.278 | 1.000 |
study will be the development of the MyCyberSkills™ iPad application prototype. This prototype will operationalize the previously developed and validated scenario-based, hands-on tasks CSI into an actual app that will be used to collect the cybersecurity skills data. Once the MyCyberSkills™ iPad app has been completed and fully tested, empirical research will be done to evaluate its reliability. Thus, the fourth objective of the larger study will be to conduct a quantitative research study using the MyCyberSkills™ iPad app by collecting data from at least 100 non-IT employees/participants and documenting the results of the measure. Results from this quantitative phase will be analyzed, reliability of the CSI will be measured, and additional adjustment to the CSI will be concluded. Recommendations for the administration as a result from the data analysis will also be provided.

ACKNOWLEDGMENT

The authors thank Dr. Gary Margules, Roxana Ross, and their team from the NSU’s Office of Research and Technology Transfer for the generous funding of this research via the NSU’s President’s Faculty and Research Development Grant (PFRDG). Moreover, the authors thank Dr. Joshua Stalker for his early contribution to this study, Dr. Eric Ackerman for his assistance with the data collection, as well as Dr. Michelle M. Ramim for her assistance and guidance during the Delphi expert panel process.

REFERENCES


