Identifying the Real Technology Skills Gap:
A Qualitative Look Across Disciplines

Evan Schirf
evan.schirf@stvincent.edu

Anthony Serapiglia
Anthony.Serapiglia@stvincent.edu

CIS Department
St. Vincent College
Latrobe, PA 15650

Abstract

Every year several survey inventories are performed throughout the IT industry by trade magazines and research groups that attempt to gauge the current state of the industry as it relates to trends. Many of these highlight a technology skills gap between job expectations and potential employees. While many job openings exist and educational programs are adjusting to produce more candidates for these jobs, many employers express dissatisfaction with the talent pool. Many of these surveys do not take into account wide differences in the spectrum of industries that employ technology workers. This study interviewed four "C" level executives from four different industries to discover more specifically which skills they have identified as being most valuable for potential employees. The results show that the "skills" gap is not just technical. The soft skills of communication, problem solving, and interpersonal skills as well as motivation and positive attitude may be more in demand than specific hard skills of programming languages or other CS/IT specific training. This may be even more pronounced in the multifaceted area of Cybersecurity.

Keywords: Skills Gap, Communication Skills, Cybersecurity, IT Education, Information Systems

1. INTRODUCTION

Computer Science and Information Technology/Systems is a very dynamic discipline both in practice and in education. One result of this dynamism is that often during cycles of change, disconnects can develop between those two areas of industry and education. Education is often looking at a much longer term picture than industry; and while the student population turns over regularly, the faculty does not. Stories of graduates leaving university unable to land jobs because of a deficit in their technological education are often reported (Allabarton, 2015; Weiner, 2014).

Security is also a moving target in both industry and education. In practice it is a constantly evolving cycle of threat re-assessment and vulnerability identification. With the specifics of the tasks in a constant state of flux, the challenge of preparing a workforce to succeed in accomplishing those tasks is also in perpetual change. It is a dynamic that has always been a challenge in the CS/IS/IT education world, how to continually keep up with the hyperactive state of change that exists in both the consumer and industrial markets. Until recently, the path to a security job in computing/information assurance/networking was through experience. It was common to see job postings that required 10 years of experience or more for anything that related to security. The positions of Chief Security

Officer (CSO) and Chief Information Security Officer (CISO) simply did not exist. In 2015, by modest estimates, more than 209,000 cybersecurity jobs in the U.S. are unfilled, and postings are up 74 percent over the past five years (Carapezza, 2015; Resa, 2014).

There is a changing atmosphere of perception and understanding of how pervasive security must be within organizations. New security personnel are expected to have the level of systemic understanding as the ten year veteran. However, most post-secondary degree and certification programs simply do not have the ability to react as quickly as the changing work environment. This inevitably results in both a real and perceived skills gap between education and industry.

A regular feature of many trade magazines is an annual survey of CIO/CSO/CISOs to assess current industry trends and to allow insight into where the skills gaps exist at that instant, as well as to help predict where they may be in the near future. While these industry surveys serve a very valuable purpose, often the quantitative results are not as insightful as they could be. Distinctions between company size and industry specialization are not often teased out from the bulk statistics.

This study set out to follow up on industry standard quantitative security surveys with qualitative interviews with four "C" level security personnel from four distinctly different industries. The purpose of these interviews and this study is to gain further insight into the differences in perspective between the four industry segments related to the technology skills gap. From these insights, specific areas may be identified to help guide changes in security curriculum to help close the current divide.

2. LITERATURE REVIEW

Industry Outlook
It is an Information Age when everyone and everything (IoT) is online, paper money is so yesterday (Bitcoin, Apple/Google Pay), and Big Data Analytics on the zettabytes of social media content generated allows marketers (and others) to know everything about their targets. As more and more data and services have moved online, so too has the recognition of the value of those things that live online electronically. With that recognition of the value of even the smallest points of data, the targeting of even the most innocuous of online material has increased. So while once the largest need were employees with the skills to build the enabling networks and

technologies of an information age/economy, the shift that has ensued now sees that the largest need are those workers skilled in knowing how maximize the potential of and to protect the systems now in use. Conventional wisdom could assume that there would simply be an overabundance of talent to be able to work with this data and function in this world. The reality of the situation, however, is far from that.

According to one 2015 study by Stanford University, more than 209,000 cybersecurity jobs in the U.S. are unfilled, and postings are up 74 percent over the past five years. The demand for positions like information security professionals is expected to grow by 53 percent through 2018 (Setalvad, 2015).

An Ernst & Young survey highlights that companies will spend marginally more money on technology and staff to defend their IT systems and data in 2015, but they continue to have problems hiring knowledgeable security professionals. "About 52 percent of the more than 1,800 organizations surveyed expect security budgets to increase, compared to 43 percent whose budgets will remain unchanged. More than half of firms identified the lack of skilled professionals as a major reason for their inability to bolster system security, according to the survey."(Ernst & Young, 2015).

In an interview with security magazine SCMagazine.com, Sean Smith director of CyberSecurityJobsite.com reports that while over 50% of the companies listing job openings on the site, only a third of the applicants are meeting the cyber security skills listed (Drinkwater, 2014).

The International Information System Security Certification Consortium, Inc., (ISC)² is one of the global leaders in educating and certifying security professionals in a variety of disciplines. The (ISC)² 2013 Global Information Security Workforce Study revealed there to be an "acute gap" between the supply and demand of qualified cyber-security professionals. It detailed there would be 3.2 million information security professionals employed in 2013, and says that this demand is growing at a compound annual growth rate (CAGR) of 11.3 percent through 2017. Some 56 percent of IT decision makers in their survey responded that they had 'too few' information security workers (Suby, 2013)

Model Curriculum
The Association for Computing Machinery (ACM) has provided model computer related curriculum

guidelines since the 1960s. The 2013 model curriculum is the latest update. In it Information Assurance and Security is broken out into it's own Knowledge Area (KA) for the first time. In defining the KA, industry standards of CIA (Confidentiality, Integrity, and Availability) are used in conjunction with providing for authentication and non-repudiation. Broadening the scope, CS2013 acknowledges that both assurance and security concepts are needed to ensure a complete perspective, "Information assurance and security education, then, includes all efforts to prepare a workforce with the needed knowledge, skills, and abilities to protect our information systems and attest to the assurance of the past and current state of processes and data (ACM, 2013)."

The model curriculum guidelines for Information Systems version 2010 lists security and risk management as one of a group of five high level IS capabilities. Under the heading of Understanding, Managing and Controlling IT Risks, this is more clearly defined as, "IS graduates should have strong capabilities in understanding, managing, and controlling organizational risks that are associated with the use of IT-based solutions (e.g., security, disaster recovery, obsolescence, etc.). At the undergraduate level, the emphasis should be on in-depth understanding of a variety of risks. Because IT solutions are so closely integrated with all aspects of a modern organization, it has become essential to manage the risks related to their use in a highly systematic and comprehensive way (ACM, 2010).

With the need to fill so many security related positions, other organizations have stepped in to begin to define what professional certifications should encompass. The International Information Systems Security Certification Consortium, (ISC)[2], was formed in 1989 as a group to determine a Common Body of Knowledge (CBK) that has become the basis for what has been the leading security certification for years, the Certified Information Systems Security Professional (CISSP) certification (ISC2, 2015). The CISSP certification includes the added requirement that not only do candidates have to pass an exam related to the CBK, but they must also show that they possess a minimum of five years of direct full-time security work experience in two or more of the security domains.

An alternative to the CISSP certification is offered by the EC-Council (The International Council of Electronic Commerce Consultants) with their flagship certification being the Certified Ethical Hacker (CEH). The CEH certificate has been offered since 2003 (Goldman, 2012) and is heavily centered on practical skills education and specifically penetration testing techniques. The name itself has been controversial, becoming both an asset and a possible hindrance to the organization and certificate holders (D'Ottavi, 2003; Olson, 2012).

The other leading organization in developing curriculum and certification programs is the SANS Institute (the name is derived from SysAdmin, Audit, Networking, and Security). Founded in 1989, the organization created their Global Information Assurance Certification (GIAC) in 1999. GIAC tests and validates the ability of practitioners in information security, forensics, and software security. SANS as an organization has grown to provide training seminars on ground and online, with the SANS Technology Institute was granted regional accreditation by the Middle States Commission on Higher Education. (SANS, 2014).

A common thread amongst these organizations in their curriculum models and certification paths, is that although both the CISSP and CEH require proof of field experience, these organizations have had a focus on providing support materials for the classroom and promoting standards of what should be included and expected of the students/certificate candidates.

3. METHODOLOGY

This project was conducted as series of interviews with current CIO/CISO or equivalent executives in order to determine what IT departments are facing in the current industry. The interviews were conducted utilizing a combination of questions culled from Harvey Nash's CIO Survey for 2015, and the CSC CIO Survey for 2014-15 (Appendix A).

The Harvey Nash CIO Survey 2015, in association with KPMG, collected data between January 6th and April 19th, 2015, and represents the views of 3,691 technology leaders from more than 50 countries, with a combined IT spend of over $200 billion. Of the respondents, 33 percent identified themselves as CIOs, nine percent as CTOs, 32 percent as director/VP in technology and the remaining 26 percent were spread between a broad range of roles including CEO, COO, CDO and senior executives (BusinessWire, 2015).

The CSC Global CIO Survey: 2014-2015 is the 6th annual barometer of CIOs' plans, priorities, threats and opportunities across nearly every industry. Almost 600 CIOs and IT leaders contributed to this report from around the world, offering insights and data to better prepare IT leaders for the challenges and possibilities of the coming years (CSC, 2015).

Questions in the interview were divided into three sections: Information Technology and Innovation, Cybersecurity, and Management of Information Systems and Personnel. Four interviews were conducted. The interviews were conducted with: 1 – IT Director of a medium sized alternative energy company, 2 – CIO of a medium sized private College, 3 – CISO of a medium sized regional retail business, 4 – Director of Security Architecture of a large national financial services banking institution.

4. RESULTS

Management of Information Systems and Personnel
The focus of this paper is on responses from the third section of the interviews relating to Management of Information Systems and Personnel. This section featured questions pertaining to how employees are being used in their department or workspace, as well as what skills the department management sees as valuable. Questions inquired as to which skills were viewed by the interviewees as overpopulated or underpopulated. The featured question of this section asked whether or not a disconnect is being seen by the interviewed CIOs or IT executives between the knowledge and skillset of new hires looking to enter the industry and the knowledge and skillset these interviewees desire to see.

Question: What are the most common day-to-day operations your department undertakes?

The responses to this question were varied and depended greatly upon the business type of the respondent.

Subject 1 simply stated that there were not day-to-day operations specifically related to IT. Where managerial office duties fell in with things like budget approvals and planning, strategic planning, invoice approvals, and employee peer reviews, IT related work was constantly rotating with ongoing projects and new projects "coming down the pipe" to the point that the respondent described his IT work as "triaging what comes across [his] desk." In contrast, Subject 2 stated his department's role in the business unit was supporting day to day operations constantly. Service operations, serving the needs of the users, such as dealing with incidents (incident management) such as troubleshooting a piece of technology and addressing overarching technical problems (problem management) through ticket creation and handling were among the common everyday activities, with long term projects with deadlines and objectives being undertaken in the background.

Subject 3, whose position was solely security focused in a stable industry, reported log management, investigating and troubleshooting alerts, dealing with malware, and reacting to things seen in logs as his department's day to day operations. Subject 4's statement of daily workload as much wider, encompassing consulting, security pattern design, vetting of current solutions, looking at capabilities matrix, creating taxonomies, understanding capabilities and applying them across the enterprise, making sure people follow appropriate governance when inserting technology into the workplace, appropriate due diligence when introducing a new security solution, management and oversight of security architecture, standards development, threat modeling, innovation activities research, and providing subject matter expertise. "So, a lot" was his summarized report.

Question: Do you believe you're experiencing a rise or fall in skills demand? Which skills do you feel are needed most/least? Which skills are overpopulated/underpopulated (in your department, in the industry)? Which skills do you personally value?

All respondents interviewed reported they were experiencing a rise in skills demand, either by direct reference or by communitive statements. While most responses differed in some way in due to different industry demands, all subjects stated they were eager to see new hires with people skills and who are, as reported by Subject 4, "as comfortable on the command line as they are in the board room" with good communication skills being the "most critical" for Subject 4 and good soft skills such as project management being needed by Subject 3. Meanwhile, most subjects offered that they were not looking for as many programming skills as they were in the past.

Subject 1 offered the observation that security skills are in huge demand, but also offered the

following statement in regards to communication skills:

"I believe there is an overpopulation of people that can code and things of that nature, but it's not a bad thing necessarily. But there's also under –and this can just be an experience thing- but there's an under population of individuals that can really take technical terms and translate that into business terms, right? I guess you could say you and I [we] could probably have a conversation about something highly technical or…very high level conversation about DHCP/TCIP, TCIP and IP Addressing and all that stuff, because someone standing there, they could be the CEO of a company, now it's going to sound like we're speaking a totally different language. But to take those concepts and ideas and translate them into something that makes sense from a business standpoint, I think that skill is very lacking... let's take someone like a coder or programmer that's going to sit there and code and program for ten, twelve, fourteen hours in front of his or her screen go home and do the same thing for another five or six hours at night. They have zero human interaction, and they don't know how to establish relationships with individuals, and I mean business relationships and manage those."

The subject then followed this statement up with an observation that too many people were coming in with coding background in the wrong languages, in that the languages new hires had experience in were not the languages he was looking for experience in.

Subject 3's responses were very similar, expressing his need for highly seasoned people with at least eight years of IT experience with both soft skills and project management skills in order to be looked at for acceptance into the subject's security department. However, the subject offered that, at least in regards to security, lots of different backgrounds were able to be utilized within the industry. He highlighted the presence of developers and managers within his security department. On the topic of what new hires had to offer, the subject had this to say:

"I can find a lot of one-off people. So if I wanted a pen tester, I could find someone to do pen testing. If I wanted a UNIX admin, I could find someone to be a UNIX admin. I don't find very many people that have

multiple skillsets or that can move between the security domains fluidly."

In regards to security specifically, the subject reported that what he called the "security boom" had taken people and made them think they are more valuable than they actually are in the industry, causing a rise in salaries and a fall in expectations.

The subject reported his personally valued skills were such skills as a good work ethic, as he stated security was not a nine-to-five job and involved many late nights, the ability to self-teach, with the added comment that he was willing to send people for training as long as they proved their worthiness for such training as well as the expansion of their own horizons on their own time, and soft skills, such as project management and the ability to work with people outside of the direct chain of command within the workplace.

Subject 4's personally valued skills were similar to Subject 3's, including a polishing technology background, a willingness to get hands dirty and be courageous, good communication skills which he valued as "critically important." The subject stated that technical skills were able to be taught through classes and certification courses, yet intangible skills such as communication and collaboration were not skills easily taught. Furthermore, the respondent stressed the need for communication skills, as many technology skills like security are embedded into everything that a company does. The subject offered that the "best security people aren't security people" but rather are the people who have an understanding of the technology or discipline in order to effectively secure it, using as an example that in order to have effective web application firewalling delivery controls, he would optimally look for someone who had been working on load balancers and application delivery controls.

The subject offered that skills that appeared "sexy" or that appeared to equate a quick pay day were overpopulated and that practical security skills were watered down in many candidates. Additionally, the subject reported that he saw skills like knowing fundamentally how technology works as underpopulated in the pool of new hires. The subject stated that technology had become "abstractions upon abstractions upon abstractions that makes things easier" and that he valued people who can "decompose complex problems into very primitive parts, and to be able to communicate that clearly and effectively."

Subject 2 responded with the statement that as his department as well as the business unit's industry was taking on more technology, there was to be a higher demand for skills to use that technology. The most of which the subject reported these to be business intelligence skills such as report generation, help desk and ticket handling, fixing overall computer problems and troubleshooting, as well as instructional designers, who are in especially high demand, that would help the transition from old technology to newer technology.

The subject reported that programming skills were on the decline due to the package availability to business units. Where in the past business units would hire programmers for in-house work, now businesses are simply using their IT staff to select and implement prepackaged software. However, the subject stated that companies will always hire network administrators, help desk people, PC technicians, business analysts, and systems analysts, yet the consistent hiring of programmers is on the decline with the exception of within the software development industry where software would be built for multiple industries. The subject highlighted the demand for people who can be business analysts that can look at the requirements for the business, select the best software package, and then help with implementation and training on said package, also suggesting that companies do not realize the value of business analysts who can look at big data and analytics like that inside an IT department, where such skills tend to fall under the category of training, which is the first place budget cuts look to for dollars.

Question: Do you see a disconnect between the knowledge and skills of new hires and the knowledge and skills you want them to have?

As the staple point of this project, this question was met with unique responses from all interviewees, where three of the four respondents reported the disconnection was not found in the difference of technical skills of the new hires versus what each interviewee wanted to see, but rather in the personal soft skills of the new hires, including their initiative, communication and collaboration skills, and patience to first learn the system before enacting change upon it.

Subject 1's response can be personified in the following statement, where he highlighted the difference in initiative that he was seeing between new hires from technical schools and those from four-year-degree, collegiate environments:

"I've seen a difference in the skillset as well as the initiative and the willing to learn more from between the individuals in these technical two-year, associate-degree type schools and a four-year collegiate school. And what I mean by that is it seems like the individuals in the 4-year college programs are more eager to learn, more well prepped for a business type of environment as well as are willing to take the initiative. Whereas someone from a technical school, a two-year trade type of school who specializes in IT or something similar, does not tend to have all the skills necessary to function in a business environment whereby a good internship would potentially help with that along with experience. Something about a four-year degree, though, it seems that doesn't seem to be the need for."

Subject 2 referenced an article in the Chronical for Higher Education, where employers reported that "recent [college] graduates often don't know how to communicate effectively, and struggle with adapting, problem-solving, and making decisions" and that graduates "dinged bachelor's-degree holders for lacking basic workplace proficiencies, like adaptability, communication skills, and the ability to solve complex problems" (Fischer, 2013). The subject commented on this article by stating that the issues addressed are not a matter the technical skills, but rather of knowing how to think in terms of written and oral communication, decision making, analytical and research skills, and the ability to solve complex problems. He offered the following statement regarding how colleges are treated in the here and now:

"When I went to college, the professor said to me, 'I'm not here to help you get a job, or to give you a skill that's going to get you a job. I'm here to educate you, teach you how to think, and expose you to a variety of things that you wouldn't get in the working world.' Now, colleges, a parent comes in admissions and says, "What's your college going to do to get my kid a job?" "What are they doing to get my kid a job?" It has evolved and changed to that."

The subject offered that the views expressed by the parents who are concerned with job acquisition are appropriate if their child is

attending a technical school, but "college is still college" where professors can teach almost anything, but they cannot teach students "how to be nice" or rather how to make students truly care about what they are doing. The subject offered that students were understanding the technical skills, but the best students are those who feel bad for showing up late to class and later to their job. And while only so many classes can be taught by colleges, the skills acquired are meant to go beyond just programming, but also include project management and coordination, which are seen often in the workplace. The subject's final response was a cautionary statement to students:

> "The worst thing you can hear from a kid,
> [is] when they have a major and they say
> 'I don't know [what I want to do].'"

Subject 4 offered that new hires simply must understand what they are working with before they can effect positive change, which requires characterizing and understanding the environment, which in turn requires patience. The subject reported that new hires are lacking in the ability to characterize and be patient with the culture they are dealing with, so much to the point of "where new hires get tripped up is by working so hard to become relevant so quickly, they quickly make themselves irrelevant", where new hires burn bridges and shatter relationships because they do not understand the culture. The subject had the following statement to offer in clarification:

> "The one thing I would tell new hires is 'it's a marathon, not a sprint.' You have to understand the organisms that you're working with and the systems that you're working with before you can effect positive change, because you, A, have to speak the language, B, be collaborative, and C, support the mission."

The subject reported the average turnaround period for a new hire to begin effecting positive change on the work environment was between three and six months, with the average falling closer to six months, where the subject does not expect a huge impact until after that "learning phase" has been gone through.

Subject 3, on the other hand, stated that there was an obvious disconnect, where new hires did not understand what it takes to be in the security industry, overvaluing their one to two years of experience displayed on their resumes. He noted the inadequacies in people's work ethic, but

focused heavier on the problem of hew hires putting flimsy or unpracticed skills on resumes as well as the number of skills displayed simply not being adequate for the job.

5. CONCLUSIONS

There is no question a gap does exist between the number of positions available and the number of available candidates to fill them. A study funded by Microsoft in 2013 reported that there are 120,000 new jobs created in the United States each year that require the skills of workers with degrees in Computer Science. However, in the US only 49,000 graduates leave university with Computer Science degrees annually creating a gap of 71,000 available jobs (Allabarton, 2015).

Many schools, colleges and universities, as well as vocational training and certification programs, have stepped up their CS/IS/IT programs to produce more and more potential employees to fill this gap.

However there are still complaints and dissatisfaction from employers as to the readiness of these potential employees. Much of the dissatisfaction has been attributed to changing skill sets and moving targets of evolving technology.

The results of this study show that this may not be the case.

From the interviews of four "C" level CS/IS/IT professionals, it can be seen that businesses, CIOs and IT executives are valuing soft skills such as communication and collaboration, in order to decompose problem solving into primitive and easily communicated parts.

While it can be frustrating to have to re-train to a specific language or software package, that process can be done rather quickly. The ability to think and act systemically, with a bigger picture in mind across departments and industries is the skill that takes far longer to obtain.

For generations, organizations emphasized in-depth domain knowledge necessary for their employee's job performance. However, a sea-change has come about in part because of the rapid transformation in workplace ambience and the far reaching effects of technology within all aspects of an organization. Among the cluster of skills that cater to this changing scenario, personality and soft skills play a major role in a person's career progress. Communication skills,

both verbal and nonverbal, problem solving skills, interpersonal skills, motivation and positive attitude are some of the most important soft skills that the organizations expect from their employees.

The soft skills surrounding the technical skills may become the deciding factors in employment decisions. Mitra (2011) says, "Attitude is a very critical personal attribute—a soft skill that exposes the real you." He adds, "There isn't any other personal attribute that is more important today than one's ethics, integrity, values and trustworthiness. One may have desirable hard skills but lack of ethics, integrity, values and trustworthiness is not taken lightly by the management of any company."

Colleges and universities can better prepare their graduates the more they can integrate experiences that emphasize these skills into their coursework. This will also lead to more satisfied employers.

6. REFERENCES

Allabarton, Rosie (2015, March 18). The skills gap is widening – but here's how you can close it. Retrieved May 14, 2016, from http://thenextweb.com/insider/2015/03/18/the-skills-gap-is-widening-but-heres-how-you-can-close-it/#gref

Bacey, C.; Warren, A. (2015, May 19). Pace of Digital Innovation Quickens; Large Companies Struggle to Keep Up, Finds Harvey Nash CIO Survey in Association With KPMG. Retrieved May 2, 2016, from http://www.businesswire.com/news/home/20150519005677/en/Pace-Digital-Innovation-Quickens-Large-Companies-Struggle

Carapezza, Kirk (2014, April 29). Poll: Skills Gap May Be Lengthening Job Searches. Retrieved February 12, 2016, from http://news.wgbh.org/post/poll-skills-gap-may-be-lengthening-job-searches

Computer Science Curricula 2013: Curriculum - ACM. (2013, December 20). Retrieved February 1, 2015, from http://ACM.ORG

CSC (2015). The CSC Global CIO Survey. Retrieved May 2, 2016, from http://www.csc.com/cio_survey_2014_2015

D'Otavi, A. (2003, February 3). Interview: Marcus J. Ranum, the "father" of the firewall. Retrieved June 4, 2015, from http://www.infoservi.it/interview-marcus-j-ranum-the-father-of-the-firewall/1057

Drinkwater, Doug (2014, March 27) More jobs but cyber security skills gap widens. Retrieved February 29, 2016, from http://www.scmagazineuk.com/more-jobs-but-cyber-security-skills-gap-widens/article/340103/

Ernst & Young (2015). Creating trust in the digital world: Global Information Security Survey 2015. Retrieved April 1, 2016, from http://www.ey.com/GL/en/Services/Advisory/ey-global-information-security-survey-2015-1

Fischer, K. (2013, March 04). The Employment Mismatch. Retrieved April 28, 2016, from http://chronicle.com/article/The-Employment-Mismatch/137625/

Goldman, J. (2012, May 2). How to Become a Certified Ethical Hacker. Retrieved April 5, 2015, from http://www.esecurityplanet.com/hackers/how-to-become-a-certified-ethical-hacker.html

Harvey Nash (2015) Harvey Nash CIO Survey 2015: Into an Age of Disruption. Retrieved May 2, 2016, from http://www.kpmg-institutes.com/content/dam/kpmg/advisory-institute/pdf/2015/harvey-nash-cio-survey-2015-full.pdf

Information Systems Curricula 2010: Curriculum - ACM. (2010, May 20). Retrieved February 1, 2015, from http://ACM.ORG

International Information Systems Security Certification Consortium. (n.d.). Retrieved June 14, 2015, from https://www.isc2.org

Mitra, Barun K. (2011). Personality Development and Soft Skills. New Delhi : OUP. Pp. 47-49

Olson, P. (2012, July 31). Exploding The Myth Of The 'Ethical Hacker' Retrieved June 3, 2015, from http://www.forbes.com/sites/parmyolson/2012/07/31/exploding-the-myth-of-the-ethical-hacker/

Resa, Dan (2014, March 1). "The Growth of Cybersecurity Jobs." Growth of Cybersecurity Jobs. Accessed May 16, 2015. http://www.burning-glass.com/research/cybersecurity/.

Setalvad, Ariha (2015, March 31). Demand to fill cybersecurity jobs booming. Retrieved April 1, 2016, from

http://peninsulapress.com/2015/03/31/cybersecurity-jobs-growth/

Suby, Michael (2013) The 2013 (ISC)2 Global Information Security Workforce Study. Retreived February 29, 2016, from https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/2013-ISC2-Global-Information-Security-Workforce-Study.pdf

Weiner, Joann (2014, September 16). The STEM paradoxes: Graduates' lack of non-technical skills, and not enough women. Retrieved May 14, 2016, from https://www.washingtonpost.com/blogs/she-the-people/wp/2014/09/26/the-stem-paradox-lack-of-skills-by-stem-graduates-and-not-enough-women/

Appendix A

The following is the survey instrument that was utilized as a base script to conduct the interviews with the four subjects that participated in this project.

A. Classification
   a. Title
      i. CIO - Chief Information Officer
      ii. IT Director
      iii. CDO - Chief Digital Officer
      iv. CISO - Chief Information Systems Officer
      v. CITO - Chief Information Technology Officer
      vi. Other (please specify)
   b. Business Type
      i. Manufacturing
      ii. Telecom
      iii. Retail/Tech/Media
      iv. Financial Services
      v. Healthcare
      vi. Government/Public Sector
      vii. Education
      viii. Other (please specify)
   c. IT Department Size
      i. Small Business: IT budget < $1M
      ii. Medium Business: IT budget $1M-$250M
      iii. Large Business: IT budget > $250M
B. Interview Questions
   a. Information Technology and Innovation
      i. What do you think is the perceived impact of IT in your organization?
      ii. What role do you feel IT plays in innovation and strategy? Does IT support or drive innovation in our organization?
      iii. Are you familiar with the term digital disruption? If you are not familiar with the term, I will provide a brief description (see page 2). How important is it to your company?
         1. 0 - Cannot say
         2. 1 - Not important at all
         3. 2 - Lowly important
         4. 3 - Moderately important
         5. 4- Highly important
         6. 5 - Crucially/Critically important
      iv. Has your industry been affected by digital disruption? If so, in what way?
      v. How do you think your business compares to current/future competitors in how it will survive or capitalize on digital disruption?
   b. Cybersecurity
      i. Do you believe your board recognizes the risks posed by cybersecurity, and do you believe it is doing enough about it?
      ii. Which department (Marketing, Financial, Legal, IT) relies the heaviest on cybersecurity?
      iii. What was the most common threat for your organization/industry in the past year or two? What do you think will be the next most common threat

within the next two years? Did you feel adequately prepared to meet past threats, and do you feel prepared to meet future threats?

    iv. CIO Magazine claims the majority of security threats are internal. Do you feel this is accurate? Are you countering this threat? If not, do you plan to pursue countermeasures against this threat?

c. Management of Information Systems and Personnel

    i. What are the most common day-to-day operations your department undertakes?

    ii. If the company wished to pursue a project that would encounter major/unsolvable problems on the IT side, how likely is your input to stop or alter the project?

    iii. What proportion of your IT department is flexible/contingent labor? If you are unfamiliar with the term, I will provide a brief description (see page 2).

    iv. Do you believe you're experiencing a rise or fall in skills demand? Which skills do you feel are needed most/least? Which skills are overpopulated/underpopulated (in your department, in the industry)? Which skills do you personally value?

       1. Harvey Nash 2015 CIO Survey claims that there is a fall in demand for skills related to business scope recognition ([1] Technical architecture, [2] Enterprise architecture, and [3] Business analysis) as well as a rise in demand for skills related to predicting change and moving on change ([1] Big data / analytics, [2] Change management, and [3] Development). Do you feel this is accurate in your organization/industry?

       2. Do you see a disconnect between the knowledge and skills of new hires and the knowledge and skills you want them to have?

(Optional) What is the oddest (most out of place for an IT worker) job or task you have had to perform to date?