Getting to know CISOs: Challenging assumptions about closing the cybersecurity skills gap

A Dissertation for the MSc in Security and Risk Management

University of Leicester, Department of Criminology

Stephen Cobb, September 2016

Abstract

Pervasive criminal abuse of information and communication technologies has increased the demand for people who can take on the task of securing organizations against the increasing scope and scale of threats. With demand for these cybersecurity professionals growing faster than the supply, a problematic "cybersecurity skills gap" threatens the ability of organizations to adequately protect the information systems upon which they, and society at large, are now heavily reliant. This dissertation focuses on one barrier to closing the cybersecurity skills gap: the current paucity of knowledge about key work roles within the cybersecurity workforce – such as Chief Information Security Officer or CISO – and questionable assumptions about what it takes to perform such roles effectively. Putting resources into closing the cybersecurity skills gap without the benefit of objective research puts those efforts at risk, a possibility that has serious negative implications for society. The dissertation employs a review of the literature to map the dimensions of the cybersecurity skills gap and identify assumptions underlying different efforts to close it. Several hypotheses are formulated regarding current assumptions about the cybersecurity workforce and then tested through a combination of secondary analysis using data from a large cybersecurity workforce survey and primary research using a smaller dataset of people employed in advanced cybersecurity roles. The results tend to confirm that cybersecurity professionals exhibit characteristics and personality traits distinct from those of other workers and other IT professionals. Also confirmed is the high value that CISOs attach to soft skills like communication, relative to technical knowledge, or even information security degrees and professional certifications. The research implies that efforts to close the cybersecurity skills gap may be imperilled by a lack of research into the personalities and characteristics of effective cybersecurity professionals. The dissertation concludes with recommendations for further work in this crucial field of study.

Keywords: cybercrime, security, skills, KSAs, FFM, workforce

Author’s Publication Notes

(The notes on this page were added to the dissertation as part of the publication process and do not appear in the original.)

This University of Leicester Department of Criminology dissertation was submitted for examination in September of 2016 in partial fulfilment of the requirements for my Master of Science in Security and Risk Management. In November, the dissertation was approved (and described by the examiners as ‘a meaningful and accessible, critically analysed report’ as well as ‘a very pleasing piece of work’). I graduated in January, 2017.

That is when I decided to make the dissertation available to the public via the Internet. My primary motive is to enable any value that this work may provide – to efforts to close the cybersecurity skills gap and advance the security profession – to be realized sooner, rather than later. After all, cybersecurity is a rapidly evolving field and the need to narrow the skills gap is urgent. Although the examiners said ‘elements of this dissertation are potentially publishable as journal articles and/or white papers’ I wanted to get the document out there in its entirety, and immediately. Of course, I may pull from, or build on, this work in peer-reviewed articles and white papers down the road, and it has already informed several conference presentations that I have delivered.

A secondary motive for publication is to provide, for anyone contemplating a programme like the MSc that I went through, a concrete sample of the type of work that this encourages and enables. That is why I have included here some of the appended elements, like the survey instrument, that often do not make it into journal articles. I did alter the formatting of the dissertation slightly, converting from A4 to US Letter (because I live in the US and know what a pain it can be to print A4 on a US printer). However, I should warn anyone quoting from this work that I left the UK spelling in place. On the plus side, in preparing the document for publication I was able to fix several typos that I missed earlier.

The degree programme itself, and my opinions about it, are the subject of several articles available online at www.CobbsBlog.com. I found the programme very rewarding, both personally and professionally, although it was challenging to complete it within the two years while keeping up with my full-time employment. I am very fortunate to work for a company (ESET) that believes in further education and offers a generous tuition reimbursement plan. While the push to complete this dissertation and the coursework that preceded it did consume many weekends and all of my paid vacation, I have to say it was worth it.

Abbreviations

(ISC)^2	International Information System Security Certification Consortium
ASVAB	Armed Services Vocational Aptitude Battery
CAP	Certified Authorization Professional
CASL	University of Maryland Center for Advanced Study of Language
CASP	CompTIA Advanced Security Practitioner
CATA	Cyber Aptitude and Talent Assessment
CCFP	Certified Cyber Forensics Professional
CCIE	Cisco Certified Internetwork Expert
CCISO	Certified Chief Information Security Officer
CCNA	Cisco Certified Network Associate
CCNP	Cisco Certified Network Professional
CEH	Certified Ethical Hacker
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CHFI	Certified Hacking Forensic Investigator
CHPSE	Certified HIPAA Privacy Security Expert
CHSE	Certified HIPAA Security Expert
CIO	Chief Information Officer
CIPM	Certified Information Privacy Manager
CIPP	Certified Information Privacy Professional
CIPT	Certified Information Privacy Technologist
CISA	Certified Information Systems Auditor
CISM	Certified Information Security Manager
CISO	Chief Information Security Officer
CISSP	Certified Information Systems Security Professional
CPTE	Certified Penetration Testing Engineer
CRISC	Certified In Risk and Information Systems Control
CSIS	Center for Strategic & International Studies
CSSLP	Certified Secure Software Lifecycle Professional
CTE	Cyber Talent Enhance or CTE, from SANS Institute
CTO	Chief Technology Officer
DCA	Digital Citizens Alliance
DoD	Department of Defense (US)
DoE	Department of Energy (US)
DoJ	Department of Justice (US)
DoL	Department of Labor (US)
ECSA	EC-Council's Certified Security Analyst
EDRP	EC-Council Disaster Recovery Professional
eNDP	eLearnSecurity Network Defense Professional
ENSA	EC-Council Network Security Administrator
EU	European Union
FBI	Federal Bureau of investigation
FFM	Five Factor Model (of personality)
GCFA	GIAC Certified Forensic Analyst

GCFA	Global Information Assurance Certification
GISF	GIAC Information Security Fundamentals
GISP	GIAC Information Security Professional
GPEN	GIAC Certified Penetration Tester
GSE	GIAC Security Expert
GWS	Global Information Security Workforce Study
GXPN	GIAC Exploit Researcher and Advanced Penetration Tester
HCISSP	HealthCare Information Security and Privacy Practitioner
I-O	Industrial and Organizational Psychology
IoT	Internet of Things
IPIP	International Personality Item Pool
KSA	Knowledge, Skill, and Ability
KSAO	Knowledge, Skill, Ability, and Other
LPT	Licensed Penetration Tester
NCJRS	National Criminal Justice Reference Service (US)
NEO	Neuroticism, Extraversion, and Openness (personality traits)
NICCS	National Initiative for Cybersecurity Careers and Studies
NICE	National Initiative for Cybersecurity Education
O*NET	Occupational Information Network (US)
OCEAN	Openness, Conscientiousness, Extraversion, Agreeableness, and Neuroticism
ONS	Office of National Statistics (UK)
OSCE	Offensive Security Certified Expert
OSCP	Offensive Security Certified Professional
OSEE	Offensive Security Exploitation Expert
OSWE	Offensive Security Web Expert
OSWP	Offensive Security Wireless Professional
PNNL	Pacific Northwest National Laboratories
RESIAC	Realistic, Investigative, Artistic, Social, Enterprising, and Conventional
SEC	US Securities and Exchange Commission
SSCP	Systems Security Certified Practitioner
STEM	Science, Technology, Engineering, and Mathematics
UK	United Kingdom
US	United States
USAF	United States Air Force

Tables and Figures

Tables

Figures

Table of Contents

Chapter 0ne: Introduction

1.1 Background and motivation

Cybercrime is a growing problem that is putting a strain on organizations of every kind in every country, impacting a significant percentage of the world's population (DCA 2016; Evans and Reeder, 2010; ONS, 2016). Businesses are heavily victimized by cybercrime, with two thirds of large UK firms detecting one or more cybersecurity breaches in the last 12 months, a quarter of those having been breached at least once a month (Klahr, Amili, Shah, Button and Wang, 2016). The cost of cybercrime has been rising year on year. In the US, the mean, annualized, per company cybercrime cost was estimated to be $15 million, based on a detailed analysis of 58 firms (Ponemon, 2015). However, assessing the exact dimensions of the global crime wave in cyberspace is beyond the scope of this dissertation, as is the determination of its root causes. The focus of this dissertation is one problematic aspect of the response to cybercrime: the cybersecurity skills gap, defined as a shortage of people with the skills required to secure information systems and data against threats to their confidentiality, integrity, and availability.

The cybersecurity skills gap can be framed in criminological terms as a shortage of *capable guardians* and the dissertation research examines assumptions about the traits and characteristics of one particular group of guardians, the people in charge of information security for the organization, often titled Chief Information Security Officer or CISO. The CISO role is effectively the pinnacle of the cybersecurity profession and so role provides a useful perspective on efforts to close the cybersecurity skills gap.

The concept of "capable guardian" plays a central role in the Routine Activity Theory of crime (Cohen and Felson, 1979; Wikström, 1995; Felson and Clarke, 1998; Pease, 2005) Routine Activity Theory was posited more than a decade before the first commercial transaction on the internet (Marshall, 2015), but Cohen and Felson presciently concluded their introduction of the theory with this observation: 'the opportunity for predatory crime appears to be enmeshed in the opportunity structure for legitimate activities' (1979: 1). Today, billions of people enjoy and rely upon legitimate activities enabled by the digital 'opportunity structure' known as the internet (BBC, 2015). Unfortunately, a growing number of them experience criminal activity that would appear to substantiate Routine Activity Theory, which holds that everyday life can create the opportunity for crimes to occur when 'motivated offenders encounter suitable targets in the absence of capable guardians' (McNeely, 2015: 31).

Although Cohen and Felson were thinking of encounters that took place in the physical world, there is ample evidence that these encounters occur in, and that Routine Activity Theory can be applied to, the virtual world of cyberspace (Newman and Clarke, 2003; Wall, 2008). Over the last ten years the vast web of interconnected information systems that form cyberspace has proven to be increasingly rich in targets, a powerful lure to likely offenders from anywhere in the physical world that has internet access (Smith, 2015).

1.2 Research focus

Unfortunately, while the suitable targets in cyberspace are many, the capable guardians are arguably too few. When it comes to fighting cybercrime, the traditional guardians of physical space, the police, are short on resources, as reported in the US (Yadron, 2014), the UK (Peachey, 2014; Ring, 2014; Ballard, 2015), Canada (Seglins and Burgess, 2015), Australia (Belot, 2016), India (Oberoi, 2016), and internationally (Interpol, 2012). As for the government's role in tracking crimes against its citizens, consider this: the year that the following headline appeared – 'Cyber-crime now included in government crime stats' – was not 1996, or even 2006, but this year (Metzger, 2016).

As with physical crime in the world of work, where much of the burden of protecting against criminal activity falls to the organization (Gill, 1994), so it is with cybercrime. To defend their systems and data against cybercriminals, many organizations employ information security professionals. According to numerous accounts and surveys, such people are in short supply. A global survey of IT spending found that nearly half (46%) of enterprises have a 'problematic shortage' of cybersecurity skills (Oltsik, 2016). A global survey of over 3,000 information security professionals in 129 countries revealed that more than one in five (86%) believed there was a shortage of skilled cybersecurity professionals (ISACA, 2015). A similar proportion in an eight nation study of 775 IT decision makers in multiple countries reported a shortage of cybersecurity skills, and many (71%) said the shortage directly and measurably damaged their organization, including reputational damage and loss of proprietary data (CSIS, 2016). Fifty-nine per cent of businesses with fewer than 500 employees contacted in an online support forum reported having no access to a security expert, not internally, nor externally via third-party contractor or managed security provider (Lemos, 2016). There is a strong case for arguing that information security efforts are being hampered by a gap between the number of people that organizations need to perform cybersecurity work and the number of people qualified to do the work, i.e. the cybersecurity skills gap.

This dissertation focuses on one barrier to the closing of the cybersecurity skills gap: the current paucity of knowledge about key work roles within the cybersecurity workforce – such as the CISO – and what it takes to perform such roles effectively (Champion, Jariwala, Ward and Cooke, 2014). Efforts to close the cybersecurity skills gap that are not guided by objective research risk wasting limited resources, a possibility that has serious negative implications for society. Even as countries around the world invest billions of dollars to increase the supply of cyber-skilled humans (White House, 2016; Curtis, 2015; Peters, 2016), there is scant evidence that these expenditures are guided by a rich understanding of the roles that need to be filled and the characteristics of those best suited to filling them (Conklin, Cline and Roosa, 2014). Indeed, several assumptions underlying efforts to close the cybersecurity skills gap appear to be flawed and are the specific target of the research presented here.

1.3 Aims and Objectives

The dissertation has two aims, the first being to identify lacunae in the literature about cybersecurity roles and the people who are needed to fill them. The second aim is to contribute to the research through analysis of both primary and secondary data with the goal of improving understanding of the traits and characteristics of one particular role, that of the CISO, the person in charge of protecting the organization's information systems. Specific objectives are to test several hypotheses related to current assumptions about cybersecurity work and the people who do it. The results are intended to inform practical recommendations for improving efforts to close the cybersecurity skills gap.

1.4 Structure of the work

Following this introduction, Chapter 2 presents a literature review that defines relevant terminology and examines existing research that is germane to the dissertation. Gaps in the research are noted, as are assumptions that are guiding various efforts at cybersecurity skills gap remediation. Different methodologies for addressing those research gaps and assessing those assumptions are explored. In Chapter 3 the design of the current study's methodology is described and testable hypotheses are formulated. Chapter 4 presents analysis of the study's quantitative data. Discussion of the findings and their implications is presented in Chapter 5. Possible limitations and ethical considerations are noted and addressed. Chapter 6 provides the dissertation's conclusion.

Chapter Two: Literature Review

2.1 Scope and objectives

This literature review begins by discussing key concepts encountered in the research and then proceeds to a survey of the evidence for a cybersecurity skills gap. Arguments about the scale and impact of the gap are considered. The review then tracks the emergence of the skills shortage, awareness of it, and responses to it, including the assumptions underlying many of those responses. Efforts to develop taxonomies of the many roles that the field of cybersecurity encompasses are examined, as is cybersecurity job analysis: research into what it takes to perform cybersecurity roles. Vocational research in related fields of endeavour that may inform efforts to close the cybersecurity skills gap is discussed. The literature review then documents the paucity of studies related to the people who constitute the cybersecurity workforce, especially the upper echelons of the profession, such as CISOs. Studies of police, military personnel, and other workers are surveyed for strategies that could be used to inform and expand research into the CISO role. Before the dissertation transitions to the consideration of research methodologies, the debate over the status of cybersecurity as a profession is assessed in terms of its potential impact on the skills gap.

2.2 Definitions

Any review of literature related to the workforce challenges posed by cybercrime's impact on cybersecurity will encounter terms that require definition. Several of these terms are defined at this point, prior to the review itself, including cybercrime, cybersecurity, KSAs and KSDAOs, soft skills, and personality.

2.2.1 Cybercrime

The concept of cybercrime is central to efforts to understand and close the cybersecurity skills gap. For the purposes of this dissertation, cybercrime is taken to mean: 'crimes in which computer networks are the target or a substantial tool' (Koops, 2011). As Wall has observed: '"cyberspace crime" would have been a more accurate descriptor'; however, he concedes that 'the term "cybercrime" prevails as the accepted term' (2008: 863). The simplicity of Koops' definition should not obscure the complexity of networks today and their scale, which extends beyond servers in data centres and workstations on company desktops to encompass not just laptops and tablets on the train or smartphones in pockets and purses, but also the Internet of Things (IoT): digital sensors, services, and apps embedded in factories, homes, hotels, planes, trains, boats, cars, lorries, and even the streets upon which they drive. Industry analysts predict that the number of networked devices that make up the digital opportunity infrastructure, each a cluster of potential attack vectors for the criminally inclined, will be in the tens of billions by 2020 (Gartner, 2015; Juniper, 2015; Cisco, 2016).

2.2.2 Cybersecurity

Like cybercrime, cybersecurity has prevailed as a term of convenience, a single word with which to denote the task of protecting the confidentiality, integrity, and availability of digital information and the systems used in its acquisition, processing, storage, and output. As such, cybersecurity is a domain within information security and information assurance. At the same time, cybersecurity encompasses information system security and Information Technology (IT) security, as well as computer security, network security, e-commerce security, e-security, and Information and Communication Technology (ICT) security.

Note that this overabundance of terminology adds to the challenge of conducting literature reviews in this field of study because multiple permutations of search terms are required to ensure that all relevant sources are identified, for example: cybersecurity workforce, IT security workforce, ICT security workforce, e-security workforce, and so on. In some contexts, notably government and military, cybersecurity is abbreviated to cyber, leading to talk of a “cyber skills gap” when referring to the cybersecurity skills gap (FEDweek, 2016). The dissertation consistently uses “cybersecurity skills gap” to avoid confusion with the alternative use of cyber skills gap to describe the general shortage of IT skills, also referred to as the IT talent gap (Goldman, 2016).

2.2.3 Skill, knowledge, ability

Even a cursory review of the cybersecurity skills gap literature reveals that its sources are diverse and varied; they include, but are not limited to, the fields of economics, industrial and organization psychology (I-O psychology), psychometrics, career studies, job analysis, law, and public policy. Fortunately, there is broad consensus that in the context of a “skills gap” the word skill refers to the combination of factors that are required to perform a particular work function, known as its KSAs, for Knowledge, Skills, and Abilities. Many organizations employ Subject Matter Experts (SMEs) to analyse KSAs at multiple points in the employment cycle: first, to analyse a job opening to determine the KSAs required to fill it; next, to measure the KSAs of prospective employees for that job to find the best candidate for it; finally, to assess performance in the job against predictors derived from steps one and two (Bennett, 1948). This work is sustained by the belief that productivity and personal happiness are both well served by a good fit between workers and the work they perform (Brayfield and Crockett, 1955; Staw, 1986; Wright and Cropanzano, 2004).

Many governments are also actively engaged in researching workforce needs. The US Department of Labor (DoL) has performed and sponsored extensive modelling of competencies for many jobs across multiple sectors. Competency in this context means the application of KSAs, or as the DoL currently defines it: ‘the capability to apply or use a set of related knowledge, skills, and abilities required to successfully perform "critical work functions" or tasks in a defined work setting’ (CareerOneStop, 2016: np).

2.2.4 Beyond KSAs

A slightly different definition of KSA, provided by the DoL in the context of cybersecurity is worth quoting because it reflects the prevailing perspective that KSAs can be acquired and can be used to measure performance:

> A cluster of related knowledge, skills, and abilities that affects a major part of one’s job (a role or responsibility), that correlates with performance on the job, that can be measured against well-accepted standards, and that can be improved through training, development, and experience (DoL, 2014: 3)

However, perceived limitations of KSAs as a predictor of job performance have led to the consideration of other factors, leading to the term KSAO, for Knowledge, Skill, Ability and Other (Neuman and Wright, 1999). The main component of “other” is personality traits (Damos, 2011).

Personality traits also enter the literature of job analysis and I-O psychology in the form of “soft skills”. According to economists Heckman and Kautz, soft skills include the following factors: ‘personality traits, goals, motivations, and preferences that are valued in the labour market, in school and in many other domains’ (2012: 451). This terminology expands skills beyond the vernacular sense of things that can be taught, but avoids any direct implication that these are inheritable qualities. A parallel can be seen in the use of the term “character trait” as employed in the literature of personality, apparently in preference to the word “character” alone, possibly because of the historical and philosophical sensitivities that surround implications of innate abilities or inherited characteristics (a topic that is beyond the scope of the dissertation, although it is worth noting that similar sensitivities figure in criminological discourse, from the days of phrenology (Beirne, 1987; Simpson, 2005) to the New Criminology critique of Eysenck’s psychology of crime (Hollin, 2007; Rafter, 2006)).

2.2.5 Personality traits

Whether they are born that way or not, different people appear to be, to varying degrees and at different times, cheerful or fearful, trusting or suspicious, caring or self-interested. These are all aspects of personality, a hotly debated and heavily researched concept in psychology in general and within I-O psychology in particular (Day and Silverman, 1989; (Cruz, Silva and Capretz, 2015). An in-depth discussion of the many different definitions of personality is beyond the scope of this dissertation, but the concept of personality traits will be considered in more detail in Chapter 3. Some researchers have studied the nexus of personality traits and cybersecurity, exploring the victimology of cyber bullying (Staude-Müller et al, 2012; Garaigordobil, 2015), and computer users who undermine security, for example by opening infectious email messages (Modic and Lea, 2012; El-Din, Halevi, Lewis and Memon, 2013; Cairns and Clark 2014). However, only three studies of the personality traits of information system defenders could be found. They will be reviewed in Chapter 3.

Given the paucity of directly relevant research, the literature of personality studies related to other types of security work was reviewed for insights on methodology and approach. Personality-oriented workforce studies were found that looked at civilian police officers (Cochrane, Tett and Vandecreek, 2003), detectives (Westera, Kebbell, Milne and Green, 2014), and military pilots (Damos, 2011). An early academic study of "police personality" found that 'good police are characterized by functional intelligence, achievement motivation, and social poise' (Hogan and Kurtines, 1975: 289). That study employed the California Psychological Inventory (CPI), an instrument that is closely related to the Minnesota Multiphasic Personality Inventory (MMPI), the psychological test most widely used for officer selection by police departments (Cochrane et al, 2003; Varela, Boccaccini, Scogin, Stump and Caputo, 2004).

Academic research into police officer personality factors has increasingly used the Five Factor Model or FFM, which describes personality as a combination of five traits (Goldberg, 1981; McCrae and Costa, 1987). The traits or domains that form the FFM, also known as the Big 5, are: Openness to experience, Conscientiousness, Extraversion, Agreeableness, and Neuroticism. Sometimes referred to by the acronym OCEAN, these traits are assessed with a questionnaire called the NEO Personality Inventory. The acronym NEO stands for the first three of the five traits that psychologists explored: Neuroticism, Extraversion, and Openness (Costa and McCrae, 1988), although early adopters referred to Neuroticism as Negative Emotionality (Howard and Howard, 1995). Big 5 studies of law enforcement personnel have tended to find high scores for Conscientiousness and low scores for Neuroticism to be good predictors of performance (Ono, Sachau, Deal, Englert and Taylor 2011). This mirrors evidence from numerous FFM studies that show these two domains to be predictive of outcomes for many aspects of life including education, earnings, criminality, longevity, and even teenage pregnancy (Borghans, Duckworth, Heckman and Ter Weel, 2008).

In a study using FFM along with cognitive ability and emotional intelligence, Ono et. al (2011) found that for their test subjects – federal criminal investigators – Neuroticism was the domain most strongly predictive of good performance. Funicelli's thesis found that the domains of Conscientiousness and Extraversion were positive performance indicators in criminal interrogators (2012). Not all studies that use FFM find a connection between personality traits and performance. In his multi-method doctoral thesis on volume crime investigators, O'Neill looked at high and low performers using the proprietary NEO PI-R UK survey package; he found no statistically significant correlations between traits and performance (2011). While an FFM study of Special Force police officers did replicate previous law enforcement research findings that showed 'police officers are highly extraverted, conscientious and emotionally stable' (Garbarino, Chiorri, Magnavita, Piattino and Cuomo, 2012: 107); the same study also found that, contrary to expectations, all officers did not share the same profile. Apparently, officers formed several different personality groups. In Sanders study of police officers with FFM, he found that 'personality characteristics had no direct bearing on individual officer performance' (2008).

On balance it seems that NEO-based personality assessment tools and the FFM have the potential to shed light on the personality traits of workers in security roles. Unfortunately, a search of the literature only located two studies that have applied FFM in a cyber-defender context (Whalen and Gates, 2007; Freed, 2014). This gap in the research will be revisited in Chapter 3.

2.3 Documenting the cybersecurity skills gap

Before reviewing any research into the nature of cybersecurity skills that might shed light on efforts to increase their supply, it is important to note that the inadequacy of that supply has not been independently documented in any peer-reviewed academic papers. The numbers cited in the Introduction come from trade organizations, industry analysts, and surveys sponsored by security companies. Clearly, the assumption that a large cybersecurity skills gap exists requires closer scrutiny, particular given the fact that the information security industry does not have the best track record when it comes to quantification (Taber, 1980; Ryan and Jefferson, 2003; Florêncio and Herley, 2013).

A prime example of numeric irresponsibility in cybersecurity is the figure of one trillion dollars reported as "the cost of cybercrime". Such numbers are often provided by organizations with a vested interest in a high number, then repeated without question or verification everywhere from newspapers and business journals to congressional hearings and the White House (Cobb, 2015). Unfortunately, politicians and the public are forced to rely on vested interests for these numbers because efforts by governments and the academy to provide objective assessments have been limited. Only one peer-reviewed study of the global cost of cybercrime has appeared to date (Anderson, Barton, Bohme, Clayton, van Eeten, Levi, Moore and Savage, 2012), and the only time that the US federal government fielded a study of the cost of cybercrime to businesses was in 2005. There are no plans to repeat that exercise and the US Department of Justice (DoJ) routinely refers requests for this type of information to private sector parties that sell cybersecurity services (see author's electronic correspondence with the National Criminal Justice Reference Service (NCJRS), Appendix E).

An analogous situation exists with regard to the size of the global cybersecurity skills gap. The widely quoted assertion that the world is 'short more than a million security professionals' comes from a report produced by Cisco, the network hardware and security vendor (Cisco, 2014: 60). No source or footnote was provided for this claim, which was presented as an estimate that had come to fruition. Nevertheless, the figure has been widely repeated, not only by journalists and industry experts (Bednarz, 2015; Morgan, 2016), but also by Cisco itself, which cited it in several further reports without further clues as to its origins (Cisco, 2015a; Cisco, 2015b).

Another widely quoted estimate of the cybersecurity gap has a slightly better provenance, having been introduced in the 2015 Global Information Security Workforce Study conducted under the auspices of (ISC)^2, one of the world's largest non-profit cybersecurity certification organizations. Known hereinafter as the GWS and conducted biannually, this study is carried out by the analyst firm Frost & Sullivan and includes responses from over 10,000 security professionals ((ISC)^2, 2011; 2013). The 2015 GWS projects that the cybersecurity skills gap will be one and a half million by 2020 ((ISC)^2, 2015). This is consistent with a gap of one million in 2014 widening at a Compound Annual Growth Rate (CAGR) of seven per cent. However, the GWS provides few details of how the projection was calculated other than to describe it as:

> the difference between Frost & Sullivan's projection of the workforce needed to fully address escalating security staffing needs and our workforce projection that accounts for workforce supply constraints (for example, a tightening labor market among security professionals) ((ISC)^2, 2015: 3).

Further evidence for the million-person cybersecurity skills shortage does exist in a 2015 report linked to Stanford University. By analysing Bureau of Labor Statistics the author determined that at least

209,000 cybersecurity jobs were unfilled in the US (Satelvad, 2015). Although Satelvad did not publish her methodology, it is possible that she extrapolated from data provided by the DoL's Occupational Information Network, known as O*NET. At the heart of O*NET is a database of hundreds of job descriptions, complete with corresponding KSAs and employment prospects. The entry for the job of Information Security Analyst states that 83,000 people held positions of this type in 2014. The entry also indicates that the expected annual growth rate for such jobs was 14 per cent or better (O*NET, 2016). Assuming a CAGR of 14 per cent and a conservative assumption that one in eight cybersecurity jobs are analyst positions, with one in four currently empty, a gap size greater than 215,000 is reached by the end of 2016. If at least 200,000 US jobs are unfilled, and one further assumption is made – that the US accounts for less than one fifth of the world's digital technology users, which is arguably a valid metric for estimating the amount of cybersecurity work that needs to be done – then a global gap of one million is quite feasible. While it has to be admitted that all of the current cybersecurity skill gap calculations fall short of academic standards, the preponderance of evidence indicates that a sizable cybersecurity skills gap does exist.

2.4 Gap awareness and job analysis

The literature review now explores how efforts to close the cybersecurity skills gap have evolved over time, thereby helping frame some hypotheses that are the focus of this dissertation. The need to develop the US cybersecurity workforce was acknowledged by the federal government even before the turn of the century (White House, 1997). The military started demanding additional cybersecurity skilled personnel after the US Air Force added cyberspace to its mission statement in 2005 (USAF, 2005).

Growing concerns over terrorism also played a role in raising questions about the supply of cyber-skilled forces. When the 8th Air Force was designated the service's new cyberspace command, it was said to be 'focused on taking the fight against terrorism to the technological realm' (Wood, 2006: np). Barely a year after the US Department of Defense (DoD) recognized cyberspace as a "warfighting domain" (USAF, 2009), Defense Secretary Robert Gates stated: 'We are desperately short of people who have capabilities in this area in all the services and we have to address it' (Real Clear Politics, 2009: np). Awareness that the skills shortage was not just one of breadth but also of depth was reflected in a report by a non-partisan, non-profit think tank that concluded:

> We not only have a shortage of the highly technically skilled people required to operate and support systems already deployed, but also an even more desperate shortage of people who can design secure systems, write safe computer code, and create the ever more sophisticated tools needed to prevent, detect, mitigate and reconstitute from damage due to system failures and malicious acts (Evans and Reeder, 2010).

That the shortage was a problem for the federal government outside the military was made clear in a study that documented the concerns of CISOs and CIOs in a wide range of agencies who complained that they were not getting enough good applicants for cybersecurity openings (PPS, 2009). Furthermore, the report noted serious workforce policy and strategy gaps, finding:

> no strategic government-wide assessment of the current state of the cybersecurity workforce …. no federal plan projecting how many cybersecurity specialists will be needed … what skills and certifications they should possess, how they should be trained, or how they should be recruited into federal service (PPS, 2009).

Since then, the US federal government has made significant efforts to address these shortcomings, partly by funding sector-specific initiatives at the Department of Energy (DoE), the DoD, and the Pentagon. The government has also responded to private sector concerns over the cybersecurity skills shortage, creating the National Initiative for Cybersecurity Education or NICE (NIST, 2014), and tasking it with improving the nation's cybersecurity education, to the benefit of both the federal workforce and the private sector (NICE, 2014).

NICE worked with public and private experts and organizations, federal agencies, and industry partners to develop the National Cybersecurity Workforce Framework (the Workforce Framework), the initial goal of which was to establish a standard taxonomy for all cybersecurity work and the workers who perform it, regardless of employer or industry sector (NICE, 2014). To accomplish this, NICE resolved cybersecurity work into 31 specialty areas organized into seven categories: Securely Provision; Operate and Maintain; Protect And Defend; Investigate; Collect And Operate; Analyze; Oversight And Development. NICE went on to identify the KSAs required for each role. For example, the work of *Investigation and Digital Forensics* contains 39 numbered task descriptions for which there are 43 KSAs (Knowledge: 25; Skill: 17; Ability: 1). Each KSA is listed with the appropriate area of competency. For example, the entry for *Knowledge of encryption algorithms* lists examples and is assigned to the *Cryptography* competency. The *Skill in performing packet-level analysis* task is assigned to the *Vulnerabilities Assessment* competency (NICE, 2014).

An impressive example of applied research, the Workforce Framework was broadly welcomed as a major improvement over the disparate ad hoc taxonomies that it sought to replace, a vital step to maturing the cybersecurity job market (Boyd, 2016). The subsequent matching of roles in the Framework with recommended credentials, suggested learning opportunities and development sources has enhanced its utility. This matching was performed by another federal government project, the National Initiative for Cybersecurity Careers and Studies (NICCS). The NICCS maintains a web-based training catalogue aligned with the Framework to help people find the education they need for specific cybersecurity roles (NICCS, 2016).

The US Department of Labor (DoL) incorporated the framework's seven categories and 31 specialty areas into a broader competency model called the *Cybersecurity Industry Model* (DoL, 2014). This starts with *Tier 1 - Personal Effectiveness Competencies* and builds from there to *Tier 5 – Industry-Sector Functional Areas*, which consists of the seven NICE categories. The DoL uses competency modelling to give employers and employees an in-depth view of what a person needs to bring to a job, such as a cybersecurity position. This shifts the focus from what defines the job to what a person needs to bring to the job. One example of research that enables this shift is a project commissioned by the DoE to address the cybersecurity workforce needs of the Smart Grid (DoE, 2016).

The Pacific Northwest National Laboratory (PNNL) study used 28 SMEs to develop a Job Analysis Questionnaire (JAQ), deployment of which identified 516 tasks that were potentially relevant to both the assessment of expertise required and the prediction of job performance (PNNL, 2012). More than one hundred "performance analysis" vignettes were generated and discussed with employees as a method of Job Performance Modelling (JPM) aimed at improving understanding of how different KSAs contributed to grid cybersecurity job performance. In its initial report on the research, PNNL outlined a three dimensional framework called the Competency box that could be used to model and track an individual's progress along a learning trajectory that went from novice to master (PNNL, 2012). This construct went beyond basic KSAs to include adult intellectual development theory (Ackerman, 1996), including notions of personality, motivation, and interests. The final project report was a body of knowledge with immediate practical value to energy sector HR professionals, recruiters, and hiring managers seeking to close the cybersecurity skills gap (O'Neil, Greitzer, Conway, Dalton, Tobey and Pusey, 2014).

2.5 Worker analysis

A clear statement of the KSAs required by a particular cybersecurity role is a vital first step towards closing the cybersecurity skills gap. Helping people find out how those KSAs can be acquired and evidenced – the appropriate education and certification – is a necessary second step. However, while the

KSAs for a particular role need to be understood, they do not describe the aptitude and personality needed to achieve success in that role, or derive satisfaction from the work it entails (Damos, 2011). Efforts to increase the number of entrants into the cybersecurity workforce may falter if these individuals do not perform well or leave due to a lack of interest in the work; in other words, if work and worker are not a good fit. The idea of fitting jobs to people and people to jobs has fascinated generations of psychologists, sociologists, economists, and other assorted academics, for over a century. This fascination extends across the private and public sectors, including the military. The US developed the Army Alpha aptitude test to assign roles to military recruits during WWI (Yoakum and Yerkes, 1920), and the US military has been a big user of aptitude tests ever since. The benefits of adult aptitude testing were articulated by one of Army Alpha's developers, two decades after its initial deployment:

> 'To forge ahead in a field of activity presupposes aptitude for it. Capacity to become proficient in the work to be done, and to find in it a certain zest, is vital to happiness and health of mind, whether in school and college, in business and government, in trade or a profession' (Bingham, 1937: 1).

Army Alpha was derived from the work of Binet, who developed the Simon-Binet intelligence test in France that formed the basis of the Stanford-Binet IQ test in the US. Other aptitude research has used Spearman's two-factor theory of abilities that sees humans as having both general cognitive ability (*g*) and specific abilities (*s*) (Spearman, 1904). To oversimplify, *s* is reflected in tests of specific abilities, like math and language, whereas *g* is the kind of general intelligence measured by an IQ test. (Note that the literature refers to *g* as Spearman's *g*, General Cognitive Ability, and GCA.) Researchers have found that humans with high *g* tend to score well on multiple tests of *s* based on statistical analysis of people at various stages of their career (Schmidt, 2002). The implication for aptitude testing is that GCA is a powerful predictor of job performance and career achievement regardless of the job, or as Schmidt put it: 'The purely empirical research evidence in I-O psychology showing a strong link between GCA and job performance is so massive that there is no basis for questioning the validity of GCA as a predictor of job performance' (2002: 207). The title of an extensive study using data from ASVAB (Armed Services Vocational Aptitude Battery) sums up this position: 'Predicting Job Performance: Not Much More than *g*' (Ree, Earles and Teachout, 1994).

Despite the popularity of standardized tests of ability and achievement some researchers contend that they do not adequately account for the role that soft skills – like personality traits and personal motivation – play in determining career success over the life cycle. As the economists Heckman and Kautz assert: 'success in life depends on many traits, not just those measured by IQ, grades, and standardized achievement tests' (2012: 37). This position is well explicated by an extensive study in which economists worked with a psychologist to document the ability of personality traits to act 'both as predictors and as causes of academic and economic success, health, and criminal activity' (Almlund, Duckworth, Heckman and Kautz, 2011: 3). Based on these findings, the dissertation will look at personality traits exhibited in the cybersecurity role of CISO with the goal of better understanding those traits that are a good fit for the role.

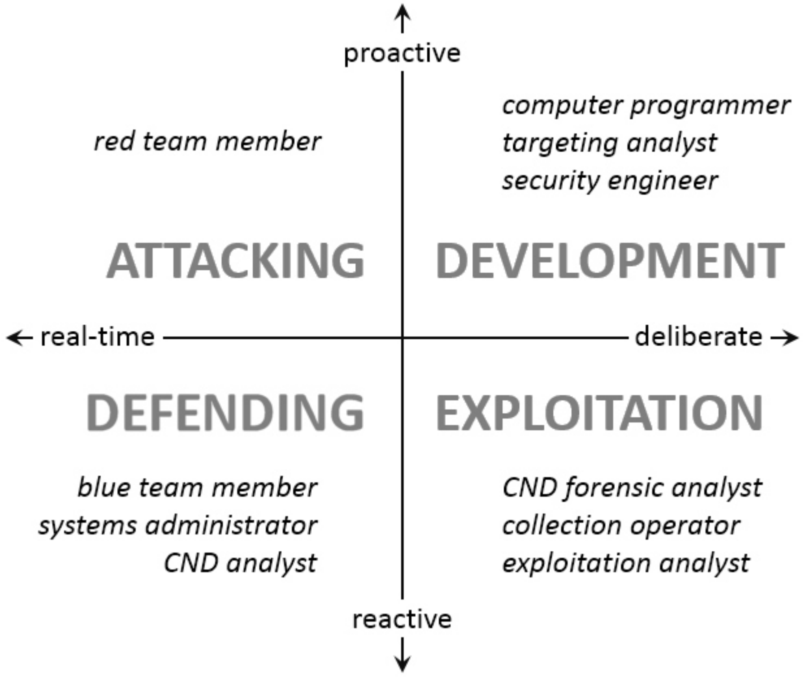
2.6 Analysing cyber workers

In the US, the armed services continue to be one of the largest users of aptitude testing. In recent years the ASVAB has been complemented by the ASVAB CT or Cyber Test. Designed to predict the performance of trainees in entry-level military roles that are cyber-related (Morris and Waage, 2015), the ASVAB CT is also an indirect measure 'of interest, intrinsic motivation, and skill in a particular area' (Trippe et al., 2015, as cited in Morris and Waage, 2015: np). In addition, the military has looked beyond ASVAB by funding research into different ways of identifying people who have what it takes to be good at cybersecurity. According to the comprehensive review by Morris and Waage, several projects show promise and are nearing maturity (2015).

One private sector initiative being tested by the military is Cyber Talent Enhance or CTE, from SANS Institute. This is a combined aptitude and skills exam designed to determine the applicant's aptitude for cyber operations as well as any cybersecurity skills they may already have (Morris and Waage, 2015). The latter is assessed using the same body of knowledge as the SANS cybersecurity training. The military is also exploring a somewhat different type of test being developed by the University of Maryland Center for Advanced Study of Language (CASL): the Cyber Aptitude and Talent Assessment (CATA). The CATA researchers decided to look at aptitude independent of current skills because the latter may become obsolete (Campbell, O'Rourke and Bunting, 2015; Campbell, Saner and Bunting, 2016).

The CATA research also captured the multi-dimensional nature of different cyber careers. Different roles can require very different requirements and CATA maps these orthogonally on the two axes of proactive/reactive and real-time/deliberate, as diagrammed in Figure 1 below (Campbell et al., 2015: 722). Note that the items in italics are representative of cybersecurity roles appropriate to each of the four quadrants. Work on the CATA is continuing under a government contract and its predictive capabilities are still being evaluated.

Figure 1: The CATA model (after Campbell et al., 2015: 722)



In practical terms, the CATA offers the military potential advantages over CTE because the latter is a proprietary instrument, charges for the use of which could quickly exceed the cost of one that the government paid to create and thus owns (Morris and Waage, 2015). However, while the military stands to reap direct benefits from its initiatives to generate cybersecurity talent ab initio, the potential of that talent to later swell the ranks of the civilian cybersecurity workforce may be limited. For the military, cyber is a domain in which the ability to attack can be as important as the ability to defend, and defensive measures can be far more aggressive than those countenanced in the civilian world, in other words it is categorically different from cybersecurity for enterprises, schools, non-profits, and NGOs. Many successful cybersecurity professionals in the private sector do have a military background, but there may be lingering concern that veterans of military action in cyberspace who transition over to securing civilian systems could be too quick to interpret attacks against them as the work of nation state actors (Robertson and Riley, 2015).

2.7 Summary

A variety of online search tools were used in the literature review. These included remote access to the University of Leicester's David Wilson Library. The following databases were also searched: ASSIA, Criminal Justice Abstracts, Google Scholar, Ingenta, the Leicester Research Archive, PsycINFO, Scopus, and Sociological Abstracts, and worldwidescience.org. A concerted search of the literature using these tools suggests there are very few peer-reviewed studies in the academic literature that address either the scale of the cybersecurity skills gap or the problem of how to close it.

Before proceeding to a consideration of methods by which gaps in the research may be remediated it should be noted that the paucity of published literature does not necessarily mean there has been a lack of engagement with the problem by academics. Some academics have worked with industry SMEs on government funded research projects that have borne fruit. As described in 2.4, there are now frameworks that provide a more granular understanding of cybersecurity work using a well-developed taxonomy. Prospective entrants into the field have ready access to a lot more information than just five years ago in terms of the KSAs required and the sources of appropriate training and education. In some sectors the efforts of the past few years have improved the ability to bring cybersecurity hires on board. Nevertheless, the number of people able to do the growing amount of cybersecurity work that needs to be done is still placing a strain on the efforts to close the gap, a phenomenon reflected in headlines like 'New computer science course's challenge is finding qualified teachers to teach it' (Maio, 2016). The current situation appears to be one in which people are too busy trying to solve a problem to adequately document the problem or question the solutions being implemented.

Chapter 3: Methodology

The shortage of academic research into the cybersecurity skills gap has not prevented extensive discourse on the subject in the mainstream press (Peterson, 2016), in the business press (Megaw, 2015), in trade magazines (Townsend, 2016), and within professional associations like the IEEE and the ACM (Platt 2015; Potter and Vickers, 2015). Unfortunately, much of this discourse, like efforts to close the gap, lacks a sound basis in academic research. Arguably, this puts at risk society's investment in expanding the cybersecurity workforce. A research methodology was needed to evaluate some of these assumptions, which are now described, together with hypotheses framed to test several of them.

3.1 Operationalization

A common assumption is that because cybersecurity career paths have been mapped out and the training and education required to follow them have been identified, enough people will now go down those paths and so the gap will soon get closed (Boyd, 2016). This assumption is often bolstered by another: a sufficient number of new entrants will take these well-charted paths because of the higher wages paid to cybersecurity workers relative to the general workforce and even some other members of the IT workforce (Libicki, Senty and Pollak, 2014). Another assumption inherent in many calls for greater efforts to close the cybersecurity skills gap is that the answer lies in more STEM education in general – graduating more students with degrees in Science, Technology, Engineering, and Mathematics – and more Computer Science degrees in particular (Wajsgras, 2016). Some politicians have gone so far as to call for cuts in liberal arts funding to increase the STEM spend (Cohen, 2016). Considerable effort has also gone into expanding the number of college graduates with information security degrees.

There are several grounds for questioning the above assumptions, not least of which is the apparent persistence of the cybersecurity skills gap in the face of considerable efforts that have already been directed at its remediation. More specifically, assumptions regarding the role of higher education in producing successful cybersecurity professionals would appear to be at odds with a relatively solid finding from the GWS as to the value of having an information security degree: it was rated last out of 12 attributes described as 'contributing to being a successful information security professional' ((ISC)^2, 2015: 25). However, if this value were found to vary according to respondent age it might be a reflection of the relative recency of such degrees. Thus, the first hypothesis of the dissertation (H1) is that the perception of an information security degree as an essential attribute of successful CISOs varies by age.

A second hypothesis suggests that an inverse of that phenomenon exists: more established members of the profession place greater value on professional certifications than newer entrants (H2). The third hypothesis questions the assumption that one particular attribute – technical knowledge – is the primary ingredient for success in the cybersecurity workforce. H3 is framed thus: cybersecurity professionals value communication skills, part of the soft skills or KSAOs, at least as much as technical knowledge. A complementary hypothesis (H4) parallels H1 in positing that the value placed on communication skills by cybersecurity professionals in general increases with length of time in the field and/or seniority within the organization's cybersecurity management.

The next three hypotheses speak to the current lack of knowledge about the people who become effective cybersecurity professionals, defined as attaining positions of responsibility for security within the organization. It is posited that such people place different values on key character traits than workers in other professional guardianship roles such as that of detective (H5). Furthermore, it is theorised that the personality of cybersecurity professionals is detectably different from that of other professionals working in IT (H6), and that cybersecurity professionals with direct responsibility for the organization's cybersecurity will be different from those who are not (H7). A final hypothesis is that US respondents to a survey about CISOs will perceive some cybersecurity issues differently from the general population (H8). The eight hypotheses are summarised in Table 1.

Table 1: Summary of 8 hypotheses about cybersecurity professionals

H1	The older ones see less value in an information security degree
H2	The more established ones see more value in certifications
H3	They all value communication skills at least as much as technical knowledge
H4	They tend to value communication skills more as they age and gain experience
H5	They value key character traits differently from other professional guardians
H6	They possess a mix of character traits that differs from other IT workers
H7	Those in the CISO role have a mix of character traits that differs from their colleagues
H8	They perceive cybersecurity challenges differently from the general population

3.2 Methodological options

Researchers investigating workforce characteristics and personalities in cybersecurity and analogous fields have employed numerous methodologies, both quantitative (Riek, Böhme and Moore, 2016) and qualitative (Botta, Werlinger, Gagné, Beznosov, Iverson, Fels and Fisher, 2007). Quantitative approaches such as a survey can be costly and a low response rate can render findings subject to the criticism that they are not generalizable (Hodkinson, 2008). Qualitative approaches are subject to a similar criticism and can take a lot of time when performed to an appropriate standard (Fielding and Thomas, 2008; Gilbert, 2008). However, qualitative research has been used to good effect in some cybersecurity-related studies; for example, Pettigrew and Ryan identify seven of these in their own qualitative study of IT security decision-making (2012). More directly qualitative methods can be used, as in the "effective SIO" study by Smith and Flanagan in the UK (2000). The "effective detective" study by Westera et al. in Australia (2014) employed a mix of qualitative and quantitative methods including semi-structured interviews, Repertory Grid Technique, and Critical Incident Technique. Some research tools combine elements of quantitative and qualitative methodology. For example, while NEO-based personality profile surveys produce a lot of data for analysis, interpretation of the data is arguably a qualitative process, albeit one that requires specific expertise (McDonald and Edwards, 2007).

For the current project it was decided that three different approaches would be used, all quantitative in their methodology. Given the considerable resources required to recruit participation from a highly specific, not to mention very busy, target demographic, the use of secondary data was considered (Allum and Arber, 2008). A large existing dataset – the almost 14,000 responses from IT professionals to the 2015 GWS survey – was identified as having the potential to shed light on the first four hypotheses if several of its questions could be subjected to secondary analysis (Westmarland, 2011). At the same time, more recent and more focused data would be helpful in confirming or refuting that analysis. A fresh survey, far more modest in scope than the GWS, was thought to be feasible as a means of acquiring this supporting data. The same survey instrument could also be used to gather personality data relevant to hypotheses five and six, and ask questions relevant to hypothesis seven.

3.3 Research design

First, permission to perform secondary analysis of the tabulated responses to the GWS 2015 survey was requested and obtained from (ISC)^2 via the consulting firm of Frost & Sullivan that administers the study for (ISC)^2. The individual responses were not available, limiting the secondary analysis to the result tables provided (of which there were 552). The answers to the two questions that might shed light on the research hypotheses (numbers 21 and 24 in the survey) were in the form of Likert scales and the Mean scores were provided (but not standard deviations). The subject matter of question 21 was designated Attributes and question 24 was designated Competencies.

Second, a survey instrument was designed to collect data on Attributes and Competencies that could be compared with that of GWS 2015, as well as the Characteristics identified in the Westera effective detective study (Westera et al. 2016), and the NEO-based personality profiles of IT workers presented in Freed's thesis (2014). The four categories of results from the survey instrument, which was dubbed the CISO Survey, are mapped to the four pieces of comparative research in Table 2. Codes were assigned to identify the areas with potential for comparative analysis.

Table 2: Research data sources and categories

	Attributes	Competencies	Characteristics	NEO Profile
GWS 2015	G15-A	G15-Co		
CISO Survey	CS-A	CS-Co	CS-Ch	CS-N
Effective Detective			ED-Ch	
Freed Thesis				FR-N

While consideration was given to conducting follow-up interviews with selected participating CISOs, these were not performed due to time and resource constraints. As a compromise, some survey questions were made open-ended, allowing for additional comments. A basic thematic analysis of these is provided in Chapter 4. There is every reason to think that qualitative research in this field, such as grounded theory based studies using in-person interviews, would add considerably to our understanding of the CISO role and its demands on the individual (Charmaz, 2014).

The decision to collect personality information with the CISO Survey was made with the intention of comparing results from a fresh sample with those obtained by Freed. Any significant differences or similarities could prove instructive; however, in line with the guidance of McDonald and Edwards, no personality analysis was undertaken by the author (2007). The fact that persons untrained in psychology can freely gather NEO personality data based on the FFM is due to the "open source" pool of questions known as IPIP for International Personality Item Pool (IPIP, 2016). Frequent testing of these items by a wide range of researchers has enabled shorter assessment instruments to be fielded while maintaining consistent results based on validated constructs (Muck, Hell and Gosling, 2007).

While the IPIP NEO Short Form is 120 items as opposed to the original 300, this was still considered too long for current purposes. Some 20 item versions have been successfully fielded (Donnellan, Oswald, Baird and Lucas, 2006), however, it was decided that 30 items would be used in the CISO Survey, enabling one item to be included for each of the six facets in each of the five domains. This would enable some comparisons to be made with the work of Freed (2014) while keeping the overall survey completion time suitably brief.

3.4 Research execution

After obtaining several hundred GWS data tables from (ISC)^2 the appropriate ones were selected for further analysis, first in Microsoft Excel, then later in IBM SPSS. It should be noted that Frost & Sullivan collected the GWS data online over a 120-day period starting in October of 2014. The company recruited participants using membership rosters from professional associations, such as (ISC)^2 itself. This leaves the results open to questions related to sample bias, but this approach to surveying is common in the world of commercial surveys, which tend to be the only data sources available if the government fails to engage in such research. At least the GWS contains a larger sample than many other studies in this field.

It was decided that the CISO Survey should also be fielded electronically, despite the not insignificant concerns surrounding this approach, including sample bias (Hine, 2008). In the end, an online survey instrument was chosen despite the drawbacks because the time and effort involved in any other form of recruitment from this demographic would have been prohibitive (based on the author's professional experience, a reputable commercial agency would charge between $15,000 and $20,000 to get 250 responses to a survey of similar scope from specific demographic such as information security professionals). To accommodate the number of questions required by the CISO Survey design, a paid Survey Monkey account was created (at the student rate). This account also enabled the survey form to be given a more professional appearance, removing a potential barrier to participation. The form was then assembled, incorporating all of the desired questions and the logic needed to implement the ethics requirement of informed participant consent. After several rounds of testing and timing the number of questions was reduced to keep the completion time below 15 minutes and the final version was fielded.

Participants were invited to visit an online portal to the survey (cisosurvey.org, see Appendix B). This "Effective CISO Survey" portal was created to make the survey appealing and accessible, yet at the same time anonymous, all while making sure that the necessary disclosures were made and participant consent was fully-informed. Logic within the Survey Monkey component, which was launched by participants from the portal over a secured internet connection, required them to confirm that they had read the information disclosure before they gave consent (Appendix C). The survey forms did not request names or email addresses but a withdrawal mechanism was provided by which a participant's unique code could be emailed to the author, prior to the survey close date, requesting deletion of their survey entry. The survey was fielded on July 7 and closed on August 15. No withdrawal requests were received, although not all participants who started the survey completed it.

To recruit participants, a form of snowball sampling was used (Sturgis, 2008). Electronic invitations to participate were extended via professional connections on LinkedIn, specifically through industry groups of which the author is a member. Other social media channels were used to inform people about the survey, including Twitter, Google Plus, and the author's blog. However, the direct link to the survey was never shared and all traffic was directed to the survey portal to insure that participants were fully aware of the nature of the survey. No incentives to participate were offered except an early look at the results prior to their publication (a specific date for which was not given).

3.5 Limitations and ethical considerations

In accordance with Department of Criminology procedures, the proposed research was submitted to the appropriate University of Leicester Ethics Sub-Committee for review and no research was attempted prior to receiving approval from the university. When the letter of approval was received (Appendix A), the caveats therein were duly noted and closely observed during the entire process of survey design, distribution, analysis, and reporting.

To ensure that the proposed research was ethical, it was designed in accordance with the six key ESRC principles of ethical research established by the Economic and Social Research Council and published in the 'ESRC Framework for research ethics: Updated January 2015' (ESRC, 2015). The rights of participants were respected and protected at all times, with the survey instrument being designed to enable anonymous submissions while also offering a right of withdrawal. All information from participants was collected over encrypted communications and stored in encrypted form on appropriately protected systems that were monitored for signs of intrusion or attempted intrusion (numerous attempted intrusions into the survey portal were detected and blocked at the network level, but no personally identifiable data was ever stored on that server and no unauthorized access was detected).

In terms of ethical risks, these were considered to be relatively low because the intended research subjects were established professionals participating voluntarily and no financial incentives were on offer or implied. Participants were promised an early look at a report of the results of the survey (this will be provided prior to any formal publication). During the survey distribution phase, the author did request assistance in snowballing the survey from several colleagues and acquaintances within the cybersecurity community, but no recompense or *quid pro quo* was offered or implied.

One potential limitation of the research became obvious after the survey launched: a low response rate. Apparently the very same cybersecurity skills gap that sparked the research has also created a serious "bandwidth" issue among members of the target audience. In other words, many CISOs are currently under-staffed because of the skills gap and thus short of time to take surveys. Compounding this problem is the large number of survey invitations that IT professionals routinely receive. The bandwidth and "survey fatigue" factors had partially been addressed by keeping the survey to under 15 minutes completion time; but despite that the number of complete responses was disappointing as it weakens the statistical validity of the results.

It is worth noting that the challenge of getting overworked professionals in the field of cybersecurity to spend time with researchers is a general one, with some serious implications for future studies. Even the GWS itself has been scaled back for its 2017 iteration (the survey instrument for this was launched while the author's CISO Survey was being conducted). The reduced 2017 GWS question set, noted by the author as a participant, may be due to complaints of survey overload from security professionals (the author was invited to participate in a dozen surveys during the time his own research was conducted – see Appendix D). A shortage of people to do the work of cybersecurity would seem to be a growing obstacle to building a better understanding of what that work entails.

Another important limitation of the research design is the use of snowball sampling, a type of non-probability, convenience sampling that not only limits the validity of any generalizations from the data but also favours people who are more engaged socially (Sturgis, 2008). Sample bias has been a persistent issue in surveys conducted within the computer security profession as responses are often limited to those people who have the time and inclination to respond, and response rates relative to a sampling frame are often not tracked (Ryan and Jefferson, 2003).

Chapter Four: Results and Analysis

4.1 Data description

The 2015 GWS survey data tables used for the secondary research were provided by Frost & Sullivan in the form of 12 Microsoft Excel spreadsheets and 12 text documents that could be read in Microsoft Word. These files tabulated 13,930 responses from IT professionals. Most respondents (70%) worked in an information security role and over half (56%) were located in North America. About one in five (20%) responses were from Europe with the rest spread across the five remaining continents (note that individual survey responses were not provided, so statistical analysis based on individual data records was not possible). Just under one third of the respondents (n = 4,550) were in their thirties, slightly more than one third (n = 4,853) were in their forties. The rest of the respondents were either under 30 (n=794) or over 49 (n = 3,733). Reflecting the profession's regrettably persistent gender imbalance, most of the respondents (90%) were male. In terms of education, most respondents had a degree (90%), with many having a degree above the bachelor level (45%). Three quarters of all survey participants held the CISSP qualification (75%). Analysis of responses to key questions will be presented after the CISO Survey data is introduced.

The CISO Survey received a total of 75 responses; however, only 56 respondents completed the entire survey including the NEO personality profile. A slightly greater number completed the sections corresponding to Attributes, Competencies, and Characteristics (n = 58). Responses were received from 12 countries, with most being from the US (n=42) followed by India (n=4). Most of the respondents held positions equivalent to CISO (n=32). Of the respondents who completed the Attributes, Competencies and Characteristics, almost two thirds were 45 years of age or older (n = 39). Almost all were male (93%). All of these respondents had at least a bachelor's degree and more than half (55%) had a master's degree or higher. Many held the CISSP qualification (74%). More than half (55%) worked at organizations with more than one thousand employees.

4.2 Attributes

Analysis of the primary and secondary data will now be presented, beginning with the Attributes, followed by Competencies, Characteristics, and the NEO personality traits. The analysis will look at the data separately and then comparatively.

4.2.1 Attributes in the GWS 2015

The primary focus of the secondary analysis of responses to the GWS 2015 survey was the question that asked respondents to rate 12 items based on the perceived value of their contribution to success as a professional in the field of information security (using a five point Likert scale). The secondary research designated these items Attributes to distinguish them from the other factors being evaluated and because the published GWS 2015 report referred to them as 'attributes' (ISC2, 2015: 24). The mean score for each Attribute is listed in Table 3 (N = 13,903, SD not available).

Note that, despite the highly technical nature of the digital assets that information security professionals are charged with protecting, those surveyed only ranked T*echnical knowledge* fourth (*M* = 4.32) as an attribute contributing to success. The soft skill attribute of *Communication skills* received the highest rating (*M* = 4.43), with *Broad understanding of the security field* a close second (*M* = 4.42).

Table 3: Attribute data from GWS 2015 (G15-A)

Attributes	**Mean**	**Rank**
Communication skills	4.43	1
Broad understanding of the security field	4.42	2
Awareness and understanding of the latest security threats	4.38	3
Technical knowledge	4.32	4
Knowledge of relevant regulatory policy	3.93	5
Security policy formulation and application	3.91	6
Leadership skills	3.89	7
Possession of an information security certification	3.76	8
Project management skills	3.65	9
Business management skills	3.54	10
Legal knowledge	3.29	11
Possession of an information security degree	3.09	12

Also ahead of Technical knowledge was *Awareness and understanding of the latest security threats* (*M* = 4.38). Right at the bottom of the list is the cornerstone of numerous public and private sector responses to the cybersecurity skills gap: *Possession of an information security degree* (*M* = 3.09). Clearly, the cybersecurity professionals who participated in the 2015 GWS study thought that such a degree was less valuable than the other attributes, including *Possession of an information security certification* (*M* = 3.76).

The published version of the 2015 GWS reported the same Attribute question with a chart that listed the items according to the percentage of respondents who ranked them as first or second. In that table, *Communication skills* were listed as second to *Broad understanding*, but with both scoring the same (90%). Analysis of the original data shows *Communication skills* was in fact marginally ahead of *Broad understanding* (90.04% v. 89.94%). All of the other Attributes in the published report were ranked as shown in Table 3. Further Secondary analysis shows that the perceived value of several of the Attributes did vary by respondent age group.

To test H1, that older information security professionals placed a lower value on information security degrees, a Pearson product-moment correlation coefficient was computed with SPSS. This indicated a negative correlation with age, *r*(4) = -.959, *p* = .041. Thus, H1 was confirmed within the GWS 2015 data. However, the correlation between age and possession of an information security certification was not found to be significant, so H2 was not proved within the GWS 2015 respondents. It appears that having an information security degree, a qualification that is relatively recent, is valued more by younger security professional, but information security certification, which is more widely held and has been available for more than 20 years (Cobb, 2016a), is broadly valued across age cohorts, ranking well above a degree.

The rankings in Table 3 provide direct evidence of the relatively higher value that cybersecurity professionals place on *Communication skills* relative to *Technical knowledge* and thus tend to support H3. Additional data pertinent to this hypothesis will be examined in a moment. Secondary analysis showed that the value placed on *Communication skills* does indeed increase with age, *r*(4) = .989, *p* = .011. This helps to confirm H4 within the GWS 2015 responses. Interestingly, an even stronger positive correlation was revealed between age and *Broad understanding*, *r*(4) = .999, *p* = .001. A negative correlation was found between age and *Business management skills*, *r*(4) = -.962, *p* = .038. A similarly negative and even stronger correlation existed between age and *Legal knowledge* , *r*(4) = -.988, *p* = .012.

To further explore attitudes to some of the key Attributes, scores were analysed relative to length of professional experience. This analysis revealed further support for H4: the value of *Communication skills* correlated significantly with length of time in the information security business, r(6) = .912, p = .011.

Even more significant was the positive connection between experience and *Technical knowledge*, $r(6)$ = .924, p = .008. The relatively low esteem afforded information security degrees by seasoned security professionals had a strong negative correlation with years of experience, $r(6)$ = -.978, p = .001.

4.2.2 Attributes in the CISO Survey

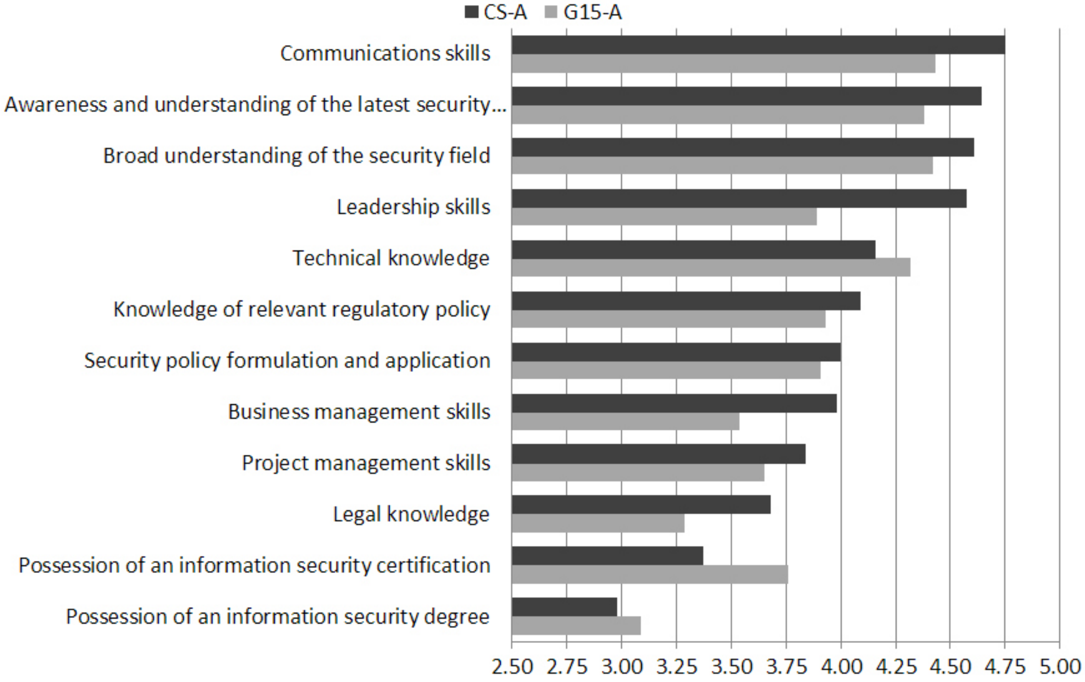
Like the GWS 2015 study, the CISO Survey found communication skills to be the most valuable attribute for success (M = 4.43), while the least valued of the listed attributes was an information security degree (M = 3.09). The median attribute scores from the CISO Survey are shown in Table 4, together with the GWS ranking for comparison.

Table 4: Attribute data from CISO Survey (CS-A)

Attributes	Mean	Rank	GWS
Communication skills	4.75	1	1
Awareness and understanding of the latest security threats	4.64	2	3
Broad understanding of the security field	4.61	3	2
Leadership skills	4.57	4	7
Technical knowledge	4.16	5	4
Knowledge of relevant regulatory policy	4.09	6	5
Security policy formulation and application	4.00	7	6
Business management skills	3.98	8	10
Project management skills	3.84	9	9
Legal knowledge	3.68	10	11
Possession of an information security certification	3.38	11	8
Possession of an information security degree	2.98	12	12

Note that the CISO Survey respondents valued *Leadership skills* over *Technical knowledge*. The latter was displaced to fifth, underlining the importance of soft skills over the types of knowledge that tend to be the focus of efforts to bolster the cybersecurity ranks. A comparison of the values from both datasets is shown in Figure 2.

Figure 2: Attribute values for CISO Survey and GWS 2015



Analysis using SPSS revealed no significant correlation between the age of the CISO Survey respondents and the value attributed to either communication skills or technical knowledge. This might be due to the fact that the far larger GWS sample was more evenly distributed across age ranges, whereas two-thirds of the CISO Survey participants were over 45. Indeed, there was only one significant correlation with age and that was *Awareness and understanding of the latest security threats*, *r*(56) =.330, *p* = .011. This is reflected in the higher mean score of this attribute, which ranked second, as can be seen in Figure 2.

4.3 Competencies

The 2015 GWS survey asked participants to rate the significance of 14 items that it referred to 'as skills and competencies in information security' and included among them two items that were specifically referred to as 'soft skills', namely: *Communication skill*s and *Analytical skills*. ((ISC)^2, 2015: 25). The scores for these competencies were subjected to secondary analysis, reported next, followed by a comparison with responses to the same question as posed in the CISO Survey.

4.3.1 Competencies in the GWS 2015

Slightly more than half the respondents of the GWS survey (n = 7,985) answered the question about how significant certain soft skills and information security competencies were in achieving their current position or level in the profession. The possible responses were: Very significant, Somewhat significant, or Not significant at all. The results were published as a per cent of survey respondents selecting Very Significant, as shown in Table 5.

Table 5: Competency data from GWS 2015 (G15-Co)

Competencies	Mean	Rank
Communications skills	77%	1
Analytical skills	75%	2
Risk assessment and management	58%	3
Governance, risk management, and compliance (GRC)	50%	4
InfoSystems and security operations management	47%	5
Incident investigation and response	41%	6
Architecture	41%	7
Platform or technology specific skills	40%	8
Engineering	31%	9
Business and business development skills	26%	10
Data administration and management	23%	11
Virtualization	21%	12
Software system development	18%	13
Acquisition/Procurement (supply chain)	8%	14

As with the GWS Attribute rankings shown earlier in Table 3, the Competency rankings place *Communication skills* above the more technical competencies such as *Architecture*, *Platform or technology specific skills*, *Engineering*, V*irtualization*, and *Software system development*. Analysis confirmed that *Communication skills* was positively correlated with age, *r*(4) = .995, *p* = .005. Several other positive correlations with age were observed, including *Analytical skills*, *GRC*, and *Risk assessment* *and management*; whereas there were strong negative correlations between age and *Acquisition/Procurement*, *Data administration*, and *Incident investigation*.

4.3.2 Competencies in the CISO Survey

Respondents to the CISO survey were presented with a soft skills and information security competencies question similar to the one that was posed in the GWS, but scored on a 5-point Likert scale (from 1 = Not at all significant to 5 = Very significant). The results, ranked by mean score, are shown in Table 6 below, together with the GWS rankings for comparison. The order of the top three entries matches the order in the GWS and places the soft skills of analysis and communication ahead of the more technical competencies. It should be noted that risk assessment and management is third in both datasets and the top rated sector-specific competency. This suggests this competency is critical to information security management (Bonney, Hayslip and Stamper, 2016).

Table 6: CISO Survey results for competencies (CS-Co)

Competencies – CISO Survey	Mean	Rank	GWS
Communications skills	4.71	1	1
Analytical skills	4.36	2	2
Risk assessment and management	4.21	3	3
InfoSystems and security operations management	4.21	4	5
Governance, risk management, and compliance (GRC)	4.05	5	4
Architecture	4.04	6	7
Incident investigation and response	3.98	7	6
Platform or technology specific skills	3.55	8	10
Business and business development skills	3.54	9	8
Data administration and management	3.36	10	11
Engineering	3.29	11	9
Acquisition/Procurement (supply chain)	3.09	12	12
Virtualization	3.02	13	13
Software system development	2.98	14	14

When the CISO Survey results for competencies were subjected to bivariate analysis in SPSS a significant correlation was seen between age and the value placed on *Communication skills*, $r(56) = .330$, $p <.011$. This finding means that data from two separate studies tend to confirm H4: the value placed on communication skills by cybersecurity professionals in general increases with length of time in the field and seniority within the organization’s cybersecurity management.

4.4 Characteristics

Earlier it was noted that, in the context of cybercrime and Routine Activity Theory, cybersecurity professionals occupy the role of capable guardians. It was hypothesized that comparing them to other capable guardians, such as law enforcement professionals, could provide insight into the qualities required to effectively fulfil the role of cyber guardian. As revealed by the literature review and discussed in the context of methodology, there have been numerous academic studies of criminal investigators and police detectives. The effective detective study by Westera et al. used qualitative methods to achieve consensus among a group of detectives ($N = 30$) on 12 ‘skill categories’ deemed most likely to differentiate effective detectives from those who are less effective (2014). Some of these items were clearly soft skills and some sounded more like personal qualities or characteristics than skills, hence the present study has designated this part of the CISO survey data as Characteristics.

While it was not possible to replicate the qualitative methods used in the Westera effective detective study in the present research, it was felt that getting a cybersecurity perspective on this set of items might be illuminating. The exact phrasing of the question in the CISO Survey was as follows: How important do you think it is for a Chief Information Security Officer to possess the following qualities? The 12 items from Westera et al. are listed in Table 7 together with the mean scores from the CISO survey respondents (*N* = 58).

Table 7: CISO Survey results for characteristics (CS-ch)

Characteristics	CISO: Mean/SD	ED: Rank
Communication	6.66	Communication
Leadership	6.55	Motivation
Decision-making	6.38	Thoroughness
Teamwork	6.32	Decision-making
Motivation	6.27	Management
Thoroughness	6.16	Experience
Resilience	6.14	Leadership
Knowledge	6.04	Knowledge
Management	6.00	Resilience
Tenacity	6.00	Tenacity
Experience	5.95	Teamwork

CISO Survey participants were asked to rate each item on a 7-point Likert scale from 1 = Not important to 7 = Very important. Also provided in the table is the ranking of these items from the effective detective study (Westera et al., 2014).

As with Attributes and Competencies, it was *Communication* that topped the list for both detectives and CISOs. However, further congruencies between the two datasets were limited, although it should be noted that *Knowledge* and *Tenacity* were near the bottom in both rankings. The variations in results from these two studies may well be due to the dissimilarities between information security work and detective work, not the least being the fact that the latter is performed as a public service, while the former is mainly conducted in the private sector (less than 30% of the CISO Survey respondents worked in either government or education). These results tend to confirm H5: cybersecurity professionals value key character traits differently from some other professional guardians.

Upon further analysis of the Characteristics data, a positive correlation was detected between age and *Communication*, *r*(56) = .369, *p* = .004. A very similar correlation was found between years of experience and *Communication*, *r*(56) = .364, *p* = .005). Taken together, these findings provide further support for H4, the tendency of information security managers to value communication skills more as they get older and have more experience.

4.5 Personality traits

During the last four decades, in dozens of studies, researchers have measured personality factors in their attempts to better understand the people who create and implement information technology (Cruz et al. 2015). Yet the personality traits of the people who defend that technology from criminal misuse and abuse do not appear to have been studied until 2004; furthermore, the results of that research were not published until 2007 (Whalen and Gates). In this study, which employed the Big 5 model that was discussed earlier in 2.2.5, participants scored high for Conscientiousness and low for Openness. The authors noted that the latter finding could imply limited ability to respond quickly to emerging security situations, but also observed that this might not be problematic because these particular study participants, attendees at a 2004 computer security conference, were less likely to be in operational roles due to the nature of the conference. Indeed, the major accomplishment of the study was to point to ways forward for future research. Sadly, such research has been slow to appear.

A personality-based study of cybersecurity team performance was published in 2015 (Cowley, Nauer and Anderson), but only one other example was located during the literature review. This was the FFM-based thesis by Freed in which the personality characteristics of cybersecurity professionals were compared to those of the general IT workforce (2014). Using the IPIP NEO Short Form, Freed found differences on six narrow traits or facets: Trust, Intellect, Vulnerability, Self Consciousness, Assertiveness, and Adventurousness (2014). That these particular differences were identified suggests that, at the very least, the personalities of cybersecurity people may differ significantly from those of other IT professionals, and thus further exploration of the personality of career information security professionals appears justified. As Freed observed, this area of research has practical implications for the workforce, such as crafting training programs that are 'specifically geared towards cybersecurity professionals' unique personality characteristics' (Freed, 2014: 40).

In an effort to evaluate the claim that cybersecurity professionals have distinctive personality profiles, the CISO Survey included a 30-item NEO profile section (see Appendix C, Question 18). Mean scores for the five OCEAN domains are listed in Table 8.

Table 8: CISO Survey OCEAN domain means compared with Freed

	CISO Survey		Freed - Cybersecurity		Freed – IT	
Domain/Facet	M	SD	M	SD	M	SD
Openness	3.708	1.088	3.442	0.551	3.254	0.478
Conscientiousness	4.039	0.923	3.932	4.047	3.866	0.555
Extraversion	3.408	1.122	3.285	0.527	3.285	0.517
Agreeableness	3.592	1.179	3.452	0.484	3.624	0.474
Neuroticism	2.313	1.235	2.589	0.552	2.713	0.625

Also listed in Table 8 are the domain means from Freed's study of cybersecurity professionals and IT professionals. Note the trend for the domains of Openness, Conscientiousness, and Neuroticism. Where Freed's scores rise from IT to Cybersecurity, the CISO Survey scores are even higher (Conscientiousness and Openness). Where Freed saw the mean for Neuroticism fall from IT to Cybersecurity, the CISO Survey mean is even lower. This could indicate that the more closely involved with cybersecurity people become the more important these domains become for success.

The CISO Survey results were explored for correlations between demographic variables and domain scores. Two of the five domains showed a statistically significant positive correlation with age: Conscientiousness $r(54) = .248$, $p = .034$ and Neuroticism $r(54) = -.343$, $p = .010$. A negative correlation was observed between length of time working as a security professional and Neuroticism $r(54) = -.330$, $p = .013$.

As was previously noted, high conscientiousness and low neuroticism have been identified as good predictors of performance in police work (Ono et al. 2011), and life in general (Borghans et al, 2009). However, some psychologists like to look beyond the domain level to the facets, for example, within the CISO Survey respondents, two facets of Conscientiousness were particularly strong: Achievement (M = 4.518) and Dutifulness (M = 4.464). Freed's cybersecurity group also had a relatively strong score for Achievement (M = 4.390), slightly less so for Dutifulness (M = 4.033). All of the OCEAN domains and corresponding facets are listed in Table 9.

Table 9: CISO Survey domain and facet means compared with Freed

		CISO		Freed - Cybersecurity		Freed – IT	
Domain/Facet		M	SD	M	SD	M	SD
O	Adventurousness	3.821	1.037	3.467	0.715	3.002	0.704
O	Artistic Interests	3.911	0.912	3.596	0.868	3.480	0.924
O	Emotionality	3.036	1.101	3.463	0.779	3.370	0.579
O	Imagination	4.107	0.748	3.460	0.942	3.345	0.885
O	Intellect	3.911	1.023	3.952	0.780	3.645	0.799
O	Liberalism	3.464	1.267	2.713	1.037	2.680	0.906
Openness		3.708		3.442		3.254	
C	Achievement	4.518	0.567	4.390	0.562	4.320	0.694
C	Cautiousness	3.696	1.101	3.854	0.828	3.760	0.912
C	Dutifulness	4.464	0.597	4.033	0.570	3.993	0.676
C	Orderliness	3.393	1.097	3.730	0.864	3.415	0.896
C	Self-Discipline	3.821	0.710	3.635	0.559	3.595	0.711
C	Self-Efficacy	4.339	0.662	4.208	0.477	4.112	0.514
Conscientiousness		4.039		3.975		3.866	
E	Activity Level	3.714	1.097	3.314	0.646	3.275	0.745
E	Assertiveness	4.071	0.776	3.893	0.730	3.535	0.694
E	Cheerfulness	3.071	1.116	3.610	0.713	3.730	0.611
E	Excitement	3.625	0.857	2.786	0.731	2.905	0.763
E	Friendliness	3.500	1.035	3.427	0.950	3.415	0.879
E	Gregariousness	2.464	1.052	2.680	0.962	2.792	0.936
Extraversion		3.408		3.285		3.275	
A	Altruism	4.286	0.647	3.996	0.715	4.030	0.599
A	Cooperation	3.286	1.359	3.824	0.738	3.945	0.824
A	Modesty	3.125	1.254	2.915	0.876	3.100	0.725
A	Morality	4.161	0.996	3.493	0.547	3.577	0.477
A	Sympathy	3.429	1.100	3.515	0.767	3.780	0.690
A	Trust	3.268	1.026	2.971	0.853	3.310	0.829
Agreeableness		3.592		3.452		3.624	
N	Anger	2.446	1.335	2.722	0.960	2.775	0.945
N	Anxiety	3.286	1.221	2.658	0.816	2.845	0.908
N	Depression	2.071	1.015	2.162	0.831	2.115	0.871
N	Immoderation	2.071	1.033	2.874	0.494	2.875	0.592
N	Self-Consciousness	2.214	1.081	2.915	0.937	3.180	0.718
N	Vulnerability	1.786	1.113	2.202	0.846	2.485	0.859
Neuroticism		2.313		2.589		2.713	

At the facet level, Freed had found that cybersecurity professionals scored significantly lower than other information technology professionals in the facets of Sympathy and Trust, and significantly higher in the facet Intellect. These are illustrated in Table 9, together with the matching results from CISO Survey profile, which recorded similar differences for Sympathy and Trust, although these were not found to be significant when analysed using the Independent T-test function in SPSS. To further explore potential differences in personality profile, the CISO Survey respondents were divided into two groups based on role: those who were CISO or similar; then the rest, dubbed non-CISOs. The Independent T-test function in SPSS did find significant differences between CISOs and non-CISOs on two of the 30 facets. For the facet Altruism, CISOs (M = 4.09, SD = .689) had significantly lower scores when compared to non-CISOs (M = 4.54, SD = .509), t(54) = -2.681, p = .010. The same was true for Self-efficacy, with CISOs (M = 4.16, SD = .723) scoring lower than non-CISOs (M = 4.58, SD = .504), t(54) = -2.475, p = .01.

4.6 Additional data points

The CISO Survey collected several additional pieces of information and these are analysed in this section before the dissertation progresses to a discussion of the findings described in the preceding sections.

4.6.1 A question of degrees

Although the 2015 GWS survey asked respondents about the value of an information security degree it did not ask whether or not participants possessed such a degree. That made it impossible to explore a fairly obvious hypothesis: that those who possess such a degree would consider it more valuable than those who do not. The CISO Survey did ask respondents to indicate if they had an information security degree and if so, did they consider it valuable. Among the respondents who answered the question (*N* = 58) about a quarter (*n* = 15) indicated they had either a Bachelors or a Masters degree in information security or both (*n* = 7).

When participants were asked to indicate the value of various Attributes, the mean score for possession of an information security degree among all respondents was 3.09 (see Table 4). The mean score among those who had such a degree was 3.33, but it was 2.85 among those who did not. While the sample size was very small and these results are thus not highly generalizable, they tend to support two hypotheses worthy of further exploration in a larger study: first, that cybersecurity professionals who have an information security degree are likely to see such a qualification as more valuable to their career than those who do not have such a degree; second, that cybersecurity professionals who have an information security degree do not see it as more valuable to their career than numerous other attributes, including professional certification.

4.6.2 Other responses

The CISO Survey questions about Attributes and Competencies offered participants an opportunity to note other factors of value or significance to the effective information security professional. Just over a third of respondents (*n* = 21) provided responses. These were numbered (*P1, P2, Pn*) and subjected to thematic analysis (Guest, MacQueen and Namey, 2011), a technique that can be used to identify concepts conveyed, either implicitly or explicitly, by textual data (Boyatiz, 1998).

The survey responses to were analysed using “open coding” (Saldana, 2013), and several themes emerged, the most notable being Humbleness. Three respondents cited humbleness or humility as being very important and another expressed sentiments thematically consistent with humbleness (P3: ‘listening to others, ability to “know what you don’t know”’).

Another clear theme was Learning (P5: ‘constant learning’; P9: ‘willingness to learn’; P17: ‘Ability to learn’). This reflected the demands inherent in another theme: Adaptability (P16: Adaptability; P17: ‘Ability to … adapt to changing threats and technology’; P5: ‘Openness to continuous process improvement’; P10: ‘Ability to … analyse DYNAMICS of the issues (i.e. not just a snapshot in time)’; P9: endless curiosity).

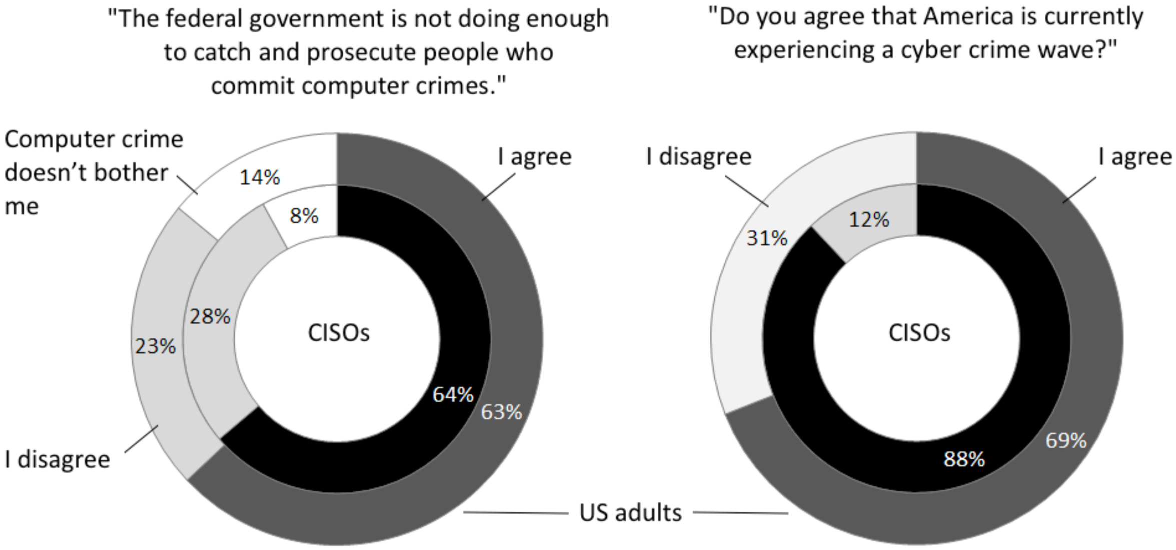
Along with Humbleness and Adaptability there was a theme of Listening (P3: ‘listening to others’; P4: ‘Listening’; P12: Community Support, All Companies/Enterprise working together, Information Sharing’). One other theme was clear: Business. This reflects the widespread notion that CISOs cannot be effective unless they can see cybersecurity as a business problem, one that cannot be addressed without understanding the business (P1: ‘a business challenge’; P7: ‘Knowledge of business operations’; P6: ‘Linking business with security’). Two other responses to the invitation to list additional factors of value are worth noting because, while they do not constitute a theme, they do serve as a reminder that CISOs can possess a sense of humour (P19: ‘Don’t be an ass’; P14: ‘Broad and deep understanding of your industry, business operations, and business model. Otherwise, you're just another guy with an opinion’).

4.6.3 Differences of opinion

In order to make the CISO Survey more enjoyable for participants, and thus more likely to be 'snowballed', two less formal questions were included. These provided an opportunity to compare the opinions of information security professionals with those of the general public on two cybersecurity-related issues, based on similar questions asked in several published national polls (Cobb, 2016b).

Early in the survey, respondents were asked if they agreed that the country was experiencing a computer crime wave. At the end of the survey they were asked to select one of three responses to this statement: The federal government is not doing enough to catch and prosecute people who commit computer crimes. The responses from US participants are reported in Figure 3 below where they are compared with results from similar questions posed in national polls of US adults.

Figure 3: CISO Survey respondents vs. general public on two issues



On the question of whether or not America is experiencing a computer crime wave, both groups agreed that it was, by a wide margin. However, note that the margin was much wider among the US CISO Survey respondents (*N* = 42).

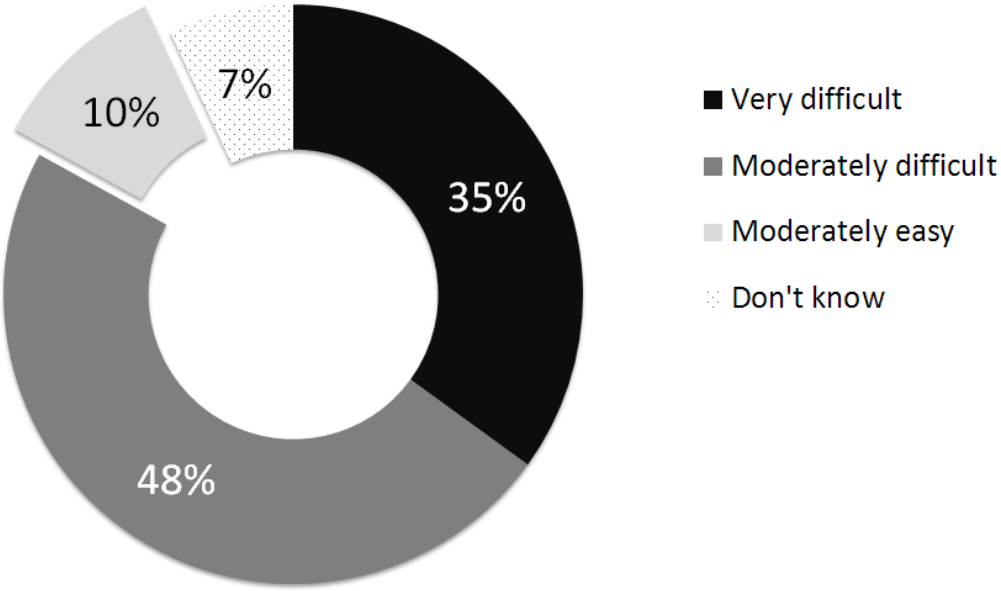
Public and CISO sentiment was more closely aligned when it came to the need for the government to do more about cybercrime. At the same time, it is clear that those who manage cybersecurity for organizations were less likely to say that they were not bothered by cybercrime.

4.6.3 The skills gap at work

The CISO Survey included one question about the skills gap itself. Respondents were asked to describe their organization's experience when it comes to hiring people for the cybersecurity roles it needs to fill. The responses are charted in Figure 4 as shown on the next page.

The available answers were: Very difficult, Moderately difficult, Moderately easy, Very easy, and Don't know. None of the respondents selected Very easy and only one in ten said hiring for cybersecurity roles was Moderately easy. About half of participants said that cybersecurity hiring was Moderately difficult (48%) and more than one third answered Very difficult. These results can be taken as further evidence that the cybersecurity skills gap is negatively impacting organizations.

Figure 4: CISO Survey views on hiring difficulty for cybersecurity roles



Note that the percentage of respondents who said hiring was either moderately or very difficult adds up to 83%. Compare this to the percentage of respondents to a contemporaneous survey of IT decision makers in multiple countries (N = 775) that admitted to a shortage of cybersecurity skills: 82% (Intel/CSIS, 2016). In that same study, 71% of respondents said that the skills shortage was responsible for “direct and measurable damage to organizations whose lack of talent makes them more desirable hacking targets”.

Chapter Five: Discussion

This chapter places the analysis of the research data in context and discusses some of the implications that it may have for the issue that is the focus of this dissertation: efforts to close the cybersecurity skills gap that threatens the security of many organizations and individuals.

5.1 Research challenges

During the last two decades the reliance on information systems and the scale and severity of attacks against them have risen to the point where cybersecurity failures pose an existential threat to organizations (SEC, 2015). In Chapter 2 it was established that the demand for cybersecurity professionals who possess the knowledge, skill, and ability necessary to defend the organization against these attacks currently exceeds the supply. It was also established that investments are being made in efforts to close this cybersecurity skills gap at all levels: global, national, regional, local, and organizational. Some individuals are also investing in their own training and education in order to enter and advance in the cybersecurity profession. Yet, as was asserted in Chapter 3, all of this activity is taking place in the absence of a solid body of objective, academically sound knowledge about what it takes to be effective as a cybersecurity professional. This creates the risk that unfounded assumptions will undermine efforts to close the skills gap and potentially produce unwanted results that impact society at large as well as individual members of the workforce.

As noted in Chapter 3, one of the challenges inherent in addressing this problematic lack of knowledge is that many of the people whom researchers need to study are too busy to be studied, because of the very skills gap on which the research is attempting to shed light. Despite this, some data was obtained for the present study, and it was analysed in Chapter 4. While the data comes with the caveats and limitations noted in Chapter 3, the results of the analysis provide potentially valuable insight into some of the aforementioned assumptions at play in efforts to address the cybersecurity skills gap.

5.2 Discussion of results

While the literature review was able to document efforts to close the cybersecurity skills gap, it found scant evidence of academic research to inform these efforts beyond the creation of a workforce framework with corresponding KSAs. Notable exceptions are the three personality studies cited earlier (Whalen and Gates, 2007; Freed, 2014; Cowley et al., 2015), and a variety of projects such as CATA that are military in their orientation (Morris and Waage, 2015). The result of this situation, as suspected at the outset of the present research project and confirmed by the results presented in Chapter 4, is that some of the common assumptions about what it takes to succeed as a cybersecurity professional are unfounded.

5.2.1 Degrees and certification

There are effective CISOs who do not have information security degrees and do not see great value in them. While younger cybersecurity professionals tend to see more value in information security degrees, as do people who have them, those degrees are generally valued less than numerous other attributes, including professional certification. Despite this, a lot of the efforts to close the cybersecurity skills gap focus on an academic path that leads to such degrees (for example, the CyberCorps Scholarship for Service program in the US is supported by 50 universities: OPM, 2016). This misalignment became apparent when the 2015 GWS was published; however it does not appear to have received much attention. This could be due to a perception of bias: how convenient that a study performed at the behest of a professional certification organization, namely (ISC)^2, found information security degrees to be less valuable than certification. However, the parallel findings from the CISO Survey argue against such bias, at least to the extent that any study based on a self-selected sample can determine.

Further evidence that information security degrees are not a powerful cure for the cybersecurity skills gap can be found in several places, starting with the 2015 GWS survey itself. Some of the results from that survey were not published, including a question asking those respondents who were responsible for hiring information security staff (N = 3,327) what importance they accorded each of four different factors when making hiring decisions: information security certifications, information security or related degree, knowledge of relevant regulator policies, or relevant information security experience. Experience emerged as the top rated factor, placing in the top two for most participants (94%). However, degrees faired worst, placed in the top spots by less than half of the respondents (46%), well below regulatory policy knowledge (65%) and certifications (70%).

Another source of possible insight into what might be called the "infosec degree dilemma" is ISACA's 2016 Cybersecurity Snapshot Global Survey which included a question about hiring new graduates for entry-level cybersecurity positions (ISACA, 2016). Almost two thirds of the respondents said it was difficult 'to identify who has an adequate level of skills and knowledge' (63%, n=2906). This could be due to one or more of several factors. The content and focus of information security degrees varies widely, from highly academic to very hands-on; or it could be that graduates are not schooled in how to convey their skills and knowledge. Furthermore, it could be argued that assessing cybersecurity skills and knowledge is inherently difficult. Whatever the actual factors at work might be, the current situation appears to be that information security degrees are not highly favoured as an indicator of potential for cybersecurity hires, at least not by cybersecurity professionals with hiring authority. This constitutes a dilemma for entrants and participants in the workforce seeking to map a career path in cybersecurity: invest several years, and possibly tens of thousands of dollars, in a degree; or opt to learn on the job and earn one or more certifications while earning money.

The infosec degree dilemma also complicates matters for the organization's human resource function, which is accustomed to screening job applications by degree status, and developing pay scales in which a degree carries considerable weight. It is important to bear in mind that even when a cybersecurity professional has hiring authority, most organizations have a hiring process that involves a human resources department, one that may not be well-equipped to identify cybersecurity talent, degreed or otherwise, a phenomenon identified and documented by PPS: 'Our surveys reveal that front-line managers are consistently less satisfied with the effort to hire new cybersecurity talent than their peers in HR' (2009: ii).

The broad support for information security certifications documented in the analysis may be due in part to the fact that, while information security degree curricula vary greatly between institutions, the specific knowledge required to obtain professional certification is typically well defined and documented in great detail. This provides a level of certainty as to what the certified cybersecurity candidate knows, a boon to the organization that is hiring and wants to know exactly what it is getting, at least in terms of a candidate's knowledge. However, in terms of providing proof of candidate skills and the ability to exercise them in practice, certifications are open to criticism due to the phenomenon of "teaching to the test" which can be seen in the many "boot camp" training offerings for security certification (Briney, 2015).

As one ISACA survey suggests, the task of evaluating the practical skills of candidates for cybersecurity roles is a difficult one (ISACA, 2016a). Another ISACA survey indicated that just over half (53%) of organizations needed at least three months to fill open cybersecurity positions (ISACA, 2016b). It could be that difficulties evaluating candidates contribute to that delay. Several approaches to addressing this aspect of the cybersecurity skills gap have been suggested, one of which is to create certifications based less on book learning than on practical tests in which skills can be demonstrated. Another approach is to borrow from the military concept of a proving ground and create cyber proving grounds where candidates could develop their skills and be tested in virtual attack and defend simulations (Alfonso, 2010). An ad hoc version of this approach has become a reality in the form of cyber defence competitions, increasingly popular in American high schools, although it is not clear whether participation in these competitions is a strong predictor of either cybersecurity as a career choice, or even performance in a cybersecurity role (Tobey, Pusey and Burely, 2014; Tobey, 2015). Some participants in these competitions could just as easily decide to become app developers or robotics engineers as cybersecurity professionals. A promising sign is the emergence of serious academic research on cyber competitors such as that by Bashir, Lambert, Wee and Guo (2015), which employed FFM in conjunction with Holland's interest classification of vocational personality types known as RIASEC for their initials: Realistic, Investigative, Artistic, Social, Enterprising, and Conventional (Fruyt and Mervielde, 1999). The study was a promising first step towards determining the potential of cyber competitions to recruit students into cybersecurity careers. Also notable is the job performance modelling work with vignettes that Tobey is adapting for talent management in cyber defence competitions (2015).

5.2.2 Communications skills and technical knowledge

Participants in the CISO Survey confirmed that communication skills are highly valued throughout the cybersecurity profession (H3); furthermore, appreciation for these skills increases as information security professionals advance in their careers (H4). However, this hardly means that technical knowledge is not important to the CISO role; a more likely interpretation is that, at this level of the cybersecurity profession, technical knowledge is a given. Indeed, technical knowledge is implicit in other highly valued attributes like awareness and understanding of the latest security threats (for example, a CISO would be expected to process news that a missing bounds check has rendered the TLS heartbeat extension vulnerable to attack, then formulate a response strategy for the organization, and explain the implications to the C-suite).

That said, information security analysts grumbling about a lack of technical knowledge at the CISO level is not unusual. This may well be due to confusion between working knowledge and the ability to acquire understanding. The scale, complexity, and speed of change of today's information systems renders a detailed working knowledge of all the ingredients all but impossible to maintain, especially if that knowledge has to coexist with awareness of business operations, customer demands, and industry regulations. What CISOs need above all is the ability to understand, evaluate, and process what they are told, while knowing whom to ask, or where to look, for the information. That ability is not only crucial to being an effective CISO, it is also a requirement for obtaining a good academic degree; in other words, it is an ability that will help a person thrive in a wide range of occupations. While this might sound at odds with the low value that CISOs appear to place on degrees (see Table 3) it could inform efforts to build a better career path for information security managers. As Campbell et al. suggested in their design goals for CATA, possession of current technical knowledge may not be a strong indicator of future cybersecurity performance, given how rapidly technology changes (2015). Imagine high school graduates going straight into the cyber workforce as entry-level technicians, acquiring security knowledge and skills on the job; then later improving their skills in analysis and communication through participation in an academic program in parallel with their continued employment. This could be a recipe for closing the cybersecurity skills while ensuring that the cybersecurity workforce has transferable skills in the event that the gap turns into a surplus (for scenarios in which this may occur see RAND, 2014).

5.2.3 Personality and character

Analysis of responses to the NEO personality questions in the CISO Survey showed an impressive consistency for some FFM domains. This would seem to confirm the research direction taken by Freed, namely to try and identify the personality traits that distinguish cybersecurity professionals in order to train them better, and potentially improve efforts to develop more of them in the workforce. Psychologists like Freed who employ personality-profiling tools such as the IPIP NEO and other psychometric tests are trained in their administration and the interpretation of their results. As McDonald and Edwards have convincingly argued, such tests are open to abuse by those not qualified to administer them (2007). For this reason the dissertation has desisted from interpreting the scores. However, even without interpretation they add to the evidence that FFM-based research could yield insights of value to efforts to close the cybersecurity skills gap. Getting that research done within the professional constraints advocated by psychologists like Edwards and McDonald is a serious challenge, but one to which it is hoped psychologists will respond positively.

Two related avenues of psychological research into worker profiles are encouraging: first, the power of soft skills relative to cognitive abilities (Heckman and Kautz, 2011); second, the economic benefits of personality psychology across society (Borghans et al.; 2008, Almlund et al., 2011). Both lines of inquiry question the immutability of personality, long considered definitional, the part of the person that persists over time. If the right circumstances and external factors can, over time, influence personality in positive ways, then the potential exists to improve the workforce, both by fostering those aspects of personality that are conducive to successful employment in more challenging roles, such as that of the CISO, as well as by increasing the supply of some highly valued soft skills, aptitude for which has traditionally been regarded as inherent.

5.3 Implications

Analysis of the GWS 2015 and CISO Survey data advanced the aims and objectives of the dissertation by providing sufficient grounds to question key assumptions at work in current efforts to close the cybersecurity skills gap, and help formulate those questions. At the same time, consideration of the existing body of literature, including workforce studies in analogous fields of endeavour, raised additional questions.

5.3.1 Questioning workforce strategies

Examination of the primary and secondary data revealed the infosec degree dilemma, a low perceived value within the industry relative to a high perceived value in society at large. It is possible to see this phenomenon as part of a larger picture, the deflation of degree value after several decades in which governments supported greatly expanded college enrolment (Owen and Sawhill, 2013). Widespread belief in the value of a degree is not surprising when the president himself has declared that going to college is “an economic imperative.” (Symonds, 2011). Fortunately, there are signs that support is growing for a blended career path, like the one briefly outlined in 5.2.2, in which the value of apprenticeship is appreciated (Howar, Mead and Seshagiri, 2016). With this approach it might be possible to reclaim the notion than an academic degree is not a vocational qualification but a way to acquire skills in communication and analysis whose value is not tied to any specific sector or technology.

5.3.2 Recommendations for further research

The world would surely welcome research efforts by its governments to more accurately assess the scale and scope of cybercrime, a leading cause of the cybersecurity skills gap. Other research questions suggested by the current study can be summarized as follows:

- For personality psychologists and proponents of the FFM: where do traits like suspicion, trust, and imagination fit in the cybersecurity personality?
- For psychologists and sociologists: why do some people seem to have a natural aptitude for, and interest in, cybersecurity? Are these innate, a product of environment, a result of life experiences, or something that can be taught?
- For sociologists and cultural historians: why do cybersecurity professionals not receive elevated social status commensurate with their role in defending the digital infrastructure that brings so many benefits to society?
- For scholars of Cultural Theory of Risk Perception and White Male Effect: could greater diversity in technology company management lead to fewer risky products entering the market, thus reducing the number of vulnerabilities for criminals to exploit?

- For researchers in I-O psychology: what is the nature of job satisfaction for cybersecurity workers? Do they face challenges akin to those experienced by other capable guardians, like burnout among police officers?
- For criminologists: is the "the crime drop" real or is it a massive case of crime displacement? Has crime simply moved, not around the corner, but into cyberspace?
- For criminologists: where does Routine Activity Theory fit in the Risk Society?

5.4 Limitations and Dissent

The size of the CISO Survey sample was disappointingly small and the means by which it was recruited are open to the criticism that it was biased and unrepresentative. The analysis of the survey responses was conducted and presented with those limitations in mind. The implications of the research were appropriately qualified and it bears repeating that this attempt to question assumptions that underpin efforts to close the cybersecurity skills gap has had to make some assumptions of its own. The unfortunate reality is that obtaining an unbiased and representative sample in this field of research is immensely challenging. Cybersecurity is a relative new and rapidly evolving field of endeavour that is currently characterized by a shortage of people, which in turns imposes serious constraints on access to those people on whom said shortage imposes demanding work schedules.

In addition to facing challenging circumstances that constrain research, the effort to close the cybersecurity skills gap must also face questions from those who think the gap is either artificial or exaggerated or both. Some of these arguments are framed in the wider context of a claimed shortage of STEM professionals (people qualified in the STEM subjects: Science, Technology, Engineering, and Mathematics). For example, it has been claimed that the current anxiety over STEM shortages is part of a recurring pattern in American business, driven in part by the reluctance of US organizations to pay the market rate for skills that are in short supply (Charette, 2016). Companies have plenty of incentive to persuade the government to pour money into creating the kind of workers they need, or provide visas so that suitably skilled workers can come to the US from other countries.

A different dynamic that may exaggerate the cybersecurity skills gap is the previously mentioned lack of appropriate hiring skills within the organization (Turgeon, 2016). This leads to "kitchen sink" job descriptions for cybersecurity roles that appear to include every known security function, representing more work than is humanely possible for one person to accomplish, however conscientious they may be. These unrealistic job descriptions result in advertisements for new hires that are often accompanied by "dream list" qualification requirements. The result is unappealing advertisements for positions that will be avoided by any cybersecurity professional who can afford to do so. More than that, companies that post such advertisements can quickly get a reputation as an organization to be avoided because it appears not to understand cybersecurity.

There is a very real sense in which, as some of this dissertation's findings indicate, the cybersecurity skills gap is the product of several other gaps, in understanding, in communication, in government responsibility, and in academic research.

Chapter Six: Conclusion

Despite the significant limitations noted in Chapters 3 and 5, it can be asserted that the dissertation has achieved its twin objectives: providing grounds for questioning several assumptions guiding efforts to close the cybersecurity skills gap; and identifying multiple gaps of a different kind, those in the cybersecurity workforce literature. The dissertation also provides evidence of how challenging it is to research a workforce that is both rapidly evolving and in short supply. While this finding helps explain those gaps in the research, that is small comfort to those who see improving the world's understanding of the cybersecurity problem as a necessary prelude to solving it. While it can be argued that the problem of crime can never be solved, it can also be asserted that the better we understand crime, the better we are able to manage it and its effects, whether through prevention, deterrence, avoidance, or insurance.

Without enough capable guardians of cyberspace, efforts to manage cybercrime are likely to fail. And the consequences of failure could be dire, with the likeliest scenario being one of the following: either the world limps along with successive generations of flawed technologies that are routinely abused by opportunistic cybercriminals; or the world's economy becomes mired in endless recession because its citizens have collectively turned their back on the productivity promised by digital technologies, the benefits of which were finally eroded to the tipping point by rampant criminal abuse.

If these scenarios seem far-fetched, consider Cohen and Felson's view that predatory crime is 'a by-product of freedom and prosperity as they manifest themselves in the routine activities of everyday life' (1979). If they are right, then cybercrime may be seen as an inevitable by-product of the digital infrastructure upon which so many hopes and dreams of freedom and prosperity have been erected, a perspective on modern life that is arguably in full accordance with that of Beck's risk society (1992).

Cyberspace would seem to be a classic case in which 'the gain in power from techno-economic "progress" is being increasingly overshadowed by the production of risks' (Beck, 1992: 13). Surely ICT and IoT belong on the list of technologies which, like nuclear power, fossil fuels, and robotics, generate risk on a global scale, creating the risk society that now defines human existence, imperilled as it is by threats of our own making (Beck, 2006; 2009). Even if the risk society perspective is rejected, there remains a strong case for saying that cybercrime is categorically different from other crime (Brenner, 2004), and that there has never been an 'opportunity structure for legitimate activities' that has embedded itself in daily life quite like the internet (Cohen and Felson, (1979: 1).

Consider the latest cause for hope in the fight against cybercrime: "next generation" security products powered by artificial intelligence (AI). These are built out of software, code that is arguably as susceptible to abuse as any other, be it the Android operating system in smartphones or the Siemens Step7 software used to program industrial control systems like those running the Iranian nuclear centrifuges, the ones that were targeted by the Stuxnet worm (Langer, 2011). These frankly Beckian problem-solution interactions have already been explored in the context of insurance (Ciborra, 2006), another human invention that has been proposed as a solution to the cybersecurity problem.

That the task of preventing predatory crime from undermining the internet-based opportunity structure is itself being undermined by a shortage of appropriately skilled people seems indisputable. Even as signs of hope appear, like elevated levels of attention paid to the problem, there are worrying indications that efforts to address it may be flawed. As the present research suggests, there appears to be a lack of due diligence on the part of those who are diverting substantial resources into luring people into the cybersecurity profession. That is, investments in cybersecurity workforce development are being made without sufficient knowledge of what it takes to succeed in this new and still evolving line of work, or what kind of people will find the work rewarding enough to continue doing it long enough to make the investment worthwhile (either to themselves personally, or to the institutions making an investment in them). The need for more research is urgent.

Acquiring the knowledge needed to efficiently and effectively close the cybersecurity skills gap will not be easy, but the stakes are high and the effort must be made. Hopefully, this work has made a useful contribution to that effort.

References

(ISC)² (2011) *2011 Global Information Security Workforce Study* (ISC)², available at: https://www.isc2.org/uploadedfiles/landing_pages/no_form/2011gisws.pdf, (accessed 25 March 2106).

(ISC)² (2013) *2013 Global Information Security Workforce Study* (ISC)², available at: https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/2013-ISC2-Global-Information-Security-Workforce-Study.pdf, (accessed 25 March 2106).

(ISC)² (2015) *2015 Global Information Security Workforce Study* (ISC)², available at: https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-(ISC)%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf, (accessed 25 March 2106).

Ackerman, P.L. (1996) 'A theory of adult intellectual development: Process, personality, interests, and knowledge', *Intelligence*, vol. 22, no. 2, 227-257.

Alfonso, K. L. (2010) 'A cyber proving ground: the search for cyber genius' *AIR UNIV MAXWELL AFB AL AIR FORCE RESEARCH INST*, available at: http://www.dtic.mil/cgi - bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA595976, (accessed 20 June 2106).

Allum, N. and Arber, S. (2008) 'Secondary Analysis of Survey Data' in N. Gilbert (ed.) *Researching Social Life* (3rd Edition), London: Sage, 372-393.

Almlund, M., Duckworth, A. L., Heckman, J. J. and Kautz, T. D. (2011) *Personality psychology and economics* (No. w16822), National Bureau of Economic Research.

Anderson, A., Barton, C., Bohme, R., Clayton, R., van Eeten, M. J. G., Levi, M., Moore, M. and Savage, S. (2012) 'Measuring the cost of cybercrime' in *11th Workshop on the Economics of Information Security (WEIS)*, available at http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf (accessed 16 April 2016).

Brenner, S. (2004) 'Cybercrime Metrics: Old Wine, New Bottles?' *Virginia Journal of Law & Technology*, **9**,13–13.

Ballard, M. (2015) 'Met Police failed on cyber crime, says top fraud officer' *Computer Weekly,* 10th June, available at: http://www.computerweekly.com/news/ 4500247897/Met-Police-failed-on-cyber-crime-says-top-fraud-officer, (accessed 23 March 2016).

Bashir, M., Lambert, A., Wee, J. M. C. and Guo, B. (2015) 'An Examination of the Vocational and Psychological Characteristics of Cybersecurity Competition' *2015 USENIX Summit on Gaming, Games, and Gamification in Security Education*, available at: https://www.usenix.org/conference/3gse15/summit-program/presentation/bashir, (accessed 1 August 2016).

BBC (2015) 'Internet used by 3.2 billion people in 2015' *BBC News*, 26th May, available at: http://www.bbc.com/news/technology-32884867, (accessed 30 July 2106).

Beck, U. (1992) *Risk society: Towards a new modernity*, London: Sage.

Beck, U. (2006) 'Living in the world risk society: A Hobhouse Memorial Public Lecture' *Economy and society*, *35*(3): 329-345.

Beck, U. (2009) *World at Risk*, Cambridge: Polity.

Bednarz, A. (2015) 'Cisco estimates a million unfilled security jobs worldwide' *Network World*, 9th March, available at: http://www.networkworld.com/article/2893365/ security0/shortage-of-security-pros-worsens.html, (accessed 3 July 2106).

Beirne, P. (1987) ‘Adolphe Quetelet and the origins of positivist criminology’ A*merican Journal of Sociology*, 1140-1169.

Belot, H. (2016) ‘Government's $230 million bid to fight cyber crime will fail without specialists, industry warns’ *Canberra Times*, 21st June, available at: http://www.canberratimes.com.au/national/public-service/governments-230-million-bid-to-fight-cyber-crime-will-fail-without-specialists-industry-warns-20160620-gpn6yz.html, (accessed 12 July 2106).

Bennett, G.K. (1948) ‘A New Era in Business and Industrial Psychology’ *Personnel Psychology*, **1**(4), 473-477.

Bingham, E. V. (1937) *Aptitudes and Aptitude Testing*, Harper Brothers, New York.

Bonney, B., Hayslip, G. and Stamper, M. (2016) *CISO Desk Reference Guide*, CISO DRG Joint Venture, San Diego.

Borghans, L., Duckworth, A. L., Heckman, J. J., and Ter Weel, B. (2008) ‘The economics and psychology of personality traits’ *Journal of human Resources*, **43**(4), 972-1059.

Botta, D., Werlinger, R., Gagné, A., Beznosov, K., Iverson, L., Fels, S. and Fisher, B. (2007) ‘Towards understanding IT security professionals and their tools’ in *Proceedings of the 3rd symposium on Usable privacy and security* (100-111), ACM.

Boyatzis, R. E. (1998) *Transforming Qualitative Information: Thematic Analysis and Code Development*, Thousand Oaks, CA: Sage.

Boyd, A (2016) ‘White House releases plan to boost cyber workforce’ *Federal Times*, 12th July, available at: http://www.federaltimes.com/story/government/cybersecurity/ 2016/07/12/cyber-workforce-strategy/86988050, (accessed 26 July 2106).

Brayfield, A.H. and Crockett, W.H. (1955) 'Employee attitudes and employee performance' *Psychological bulletin,* **52**(5) 396-424.

Briney, A. (2015) ‘First person: Editor Andrew Briney on how to pass the CISSP exam’ *SearchSecurity*, available at: http://searchsecurity.techtarget.com/feature/First-person-Editor-Andrew-Briney-on-how-to-pass-the-CISSP-exam, (accessed 30 August 2016).

Campbell, S. G., O’Rourke, P. and Bunting, M.F. (2015) ‘Identifying Dimensions of Cyber Aptitude The Design of the Cyber Aptitude and Talent Assessment’ *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Vol. 59.

Campbell, S. G., Saner, L. D., and Bunting, M. F. (2016) ‘Characterizing cybersecurity jobs: applying the cyber aptitude and talent assessment framework’ in *Proceedings of the Symposium and Bootcamp on the Science of Security*, April, ACM: 25-27.

CareerOneStop (2016) *Cybersecurity Competency Model,* available at http://www.careeronestop.org/competencymodel/competency-models/cybersecurity.aspx, (accessed 15 July 2016).

Champion, M., Jariwala, S., Ward, P. and Cooke, N.J. (2014) ‘Using Cognitive Task Analysis to Investigate the Contribution of Informal Education to Developing Cyber Security Expertise’ in *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 58, No. 1, 310-314). SAGE Publications.

Charette, R.N. (2016) 'The STEM Anxiety Business' *Computer,* **49**(3), 82-87.

Charmaz, K. (2014) *Constructing Grounded Theory* (2nd Edition), Sage: London.

Ciborra, C. 2006 ‘Imbrication of representations: Risk and digital technologies’ *Journal of Management Studies*, *43*(6), 1339-1356, available at http://paul-hadrien.info/backup/LSE/IS%20490/utile/ciborra%20risk%20and%20representation.pdf, (accessed on 29 August, 2016).

Cisco (2014) *Cisco 2014 Annual Security Report*, available at: http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf, (accessed 10 June 2106).

Cisco (2015a) *Mitigating the Cybersecurity Skills Shortage*, available at: http://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-talent.pdf, (accessed 10 June 2106).

Cisco (2015b) *Cisco 2015 Annual Security Report*, available [gated] at: http://www.cisco.com/web/offers/lp/2015-annual-security-report/index.html, (accessed 10 June 2106).

Cisco (2016) *VNI Global IP Traffic Forecast, 2015-2020*, available at: http://www.cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/index.html, (accessed 30 August 2016).

Cobb, S. (2015) 'Sizing Cybercrime: Incidents and accidents, hints and allegations' *Virus Bulletin*, available at: https://www.virusbulletin.com/uploads/pdf /conference/vb2015/Cobb-VB2015.pdf, (accessed 25 June 2106).

Cobb, S. (2016a) 'What the CISSP? 20 years as a Certified Information Systems Security Professional' *We Live Security*, 28th May, available at: http://www.welivesecurity.com/2016/05/28/cissp-certified-information-systems-security-professional, (accessed 25 June 2106).

Cobb, S. (2016b) 'Surveys galore: cybercrime wave, government prodding, and more' *S. Cobb on Security*, 2nd September, available at: http://scobbs.blogspot.com/ 2016/09/surveys-galore-cybercrime-wave.html, (accessed 2 September 2106).

Cochrane, R.E., Tett, R.P. and Vandecreek, L. (2003) 'Psychological Testing and the Selection of Police Officers: A National Survey' *Criminal Justice and Behavior,* **30**(5), 511-537.

Cohen, L.E. and Felson, C. (1979) 'Social Change and Crime Rate Trends: A Routine Activity Approach' *American Sociological Review*, Vol. 44 (August): 588-608.

Cohen, P. (2016) 'A Rising Call to Promote STEM Education and Cut Liberal Arts Funding' *New York Times*, 22nd Feb, available at: http://www.nytimes.com/2016/02/22/ business/a-rising-call-to-promote-stem-education-and-cut-liberal-arts-funding.html?_r=0, (accessed 23 July 2106).

Conklin, W. A., Cline, R. E. and Roosa, T. (2014) 'Re-engineering cybersecurity education in the us: An analysis of the critical factors' in *2014 47th Hawaii International Conference on System Sciences*, IEEE: 2006-2014.

Costa, P. T., and McCrae, R. R. (1988) 'Personality in adulthood: a six-year longitudinal study of self-reports and spouse ratings on the NEO Personality Inventory' *Journal of personality and social psychology*, **54**(5), 853.

Cowley, J.A., Nauer, K.S. and Anderson, B.R. (2015) 'Emergent Relationships between Team Member Interpersonal Styles and Cybersecurity Team Performance' *Procedia Manufacturing,* **3**, 5110-5117.

Cruz, S., da Silva, F. Q., and Capretz, L. F. (2015) 'Forty years of research on personality in software engineering: A mapping study' *Computers in Human Behavior*, 46, 94-113.

CSIS (2016) *Hacking the Skills Shortage: A study of the international shortage in cybersecurity skills*, Center for Strategic International Studies and Intel/McAfee, available at http://www.mcafee.com/us/resources/reports/rp-hacking-skills-shortage.pdf, (accessed July 15 2016).

Curtis, J. (2015) 'UK Gov will double cybersecurity funding to fend off "ISIS cyber attacks"' *IT Pro UK*, November 17, available at: http://www.itpro.co.uk/security/ 25611/uk-gov-will-double-cybersecurity-funding-to-fend-off-isis-cyber-attacks, (accessed 3 July 2106).

Damos, D. (2011) 'KSAOs for military pilot selection: A review of the literature (AFCAPS-FR-2011-0003)' Randolph AFB, TX: HQ AFPC/DSYX Strategic Research and Assessment Branch.

Day, D. V., and Silverman, S. B. (1989) ‘Personality and job performance: Evidence of incremental validity’ *Personnel Psychology* (1), 25-36.

DCA (2016) *Under Cyber Siege: Nearly Half of Americans Report Being Victims of Scam or Fraud; Majority Say Internet Has Become Less Safe, New Digital Citizens Alliance Survey Finds* [press release] available at: http://www.prnewswire.com/news-releases/under-cyber-siege-nearly-half-of-americans-report-being-victims-of-scam-or-fraud-majority-say-internet-has-become-less-safe-new-digital-citizens-alliance-survey-finds-300310192.html (access August 10 2016).

DoE Smart Grid (2016) website, available at: http://energy.gov/oe/services/technology-development/smart-grid, (accessed 2 August 2106).

DoL (2014) *Cybersecurity Industry Model: June 2104*, available at: http://www.careeronestop.org/competencymodel/competency-models/cybersecurity.aspx, (accessed 1August 2016).

Donnellan, M.B., Oswald, F.L., Baird, B.M. and Lucas, R.E. (2006) ‘The Mini-IPIP Scales: Tiny-Yet-Effective Measures of the Big Five Factors of Personality’ *Psychological assessment*, vol. 18, no. 2, 192-203.

El-Din, R. S., Cairns, P., and Clark, J. (2014) ‘Mobile Users' Strategies for Managing Phishing Attacks’ *Journal of Management and Strategy*, *5*(2), 70.

ESRC (2015) ‘ESRC Framework for research ethics: Updated January 2015’ *Economic and Social Research Council*, available at: http://www.esrc.ac.uk/files/funding/guidance-for-applicants/esrc-framework-for-research-ethics-2015, (accessed 5 December 2016).

Evans, K. and Reeder, F. (2010) ‘A human capital crisis in cybersecurity: A report of the CSIS commission on cybersecurity for the 44th presidency’ *Center for Strategic & International Studies*, available at: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/100720_Lewis_HumanCapital_WEB_BlkWhteVersion.pdf, (accessed 3 May 2106).

FEDweek (2016) ‘Report Calls for More Action on Cyber Skills Gap, *FEDweek*, 15th July, available at: http://www.fedweek.com/federal-managers-daily-report/report-calls-action-cyber-skills-gap/, (accessed 16 July 2016).

Felson M, and Clarke R. V. (1998) *Opportunity Makes the Thief: Practical Theory for Crime Prevention*. Police Research Series, Paper 98. Home Office, London.

Fielding, N. and Thomas, H. (2008) ‘Qualitative Interviewing’ in N. Gilbert (ed.) *Researching Social Life* (3rd Edition), London: Sage, 245-265.

Florêncio, D., and Herley, C. (2013) ‘Sex, lies and cyber-crime surveys’, in *Economics of information security and privacy III*, New York: Springer 35-53, http://research.microsoft.com/pubs/149886/SexLiesandCybercrimeSurveys.pdf (accessed 10 January 2015).

Freed, S. E. (2014) *Examination of personality characteristics among cybersecurity and information technology professionals*, University of Tennessee Masters Thesis, available at: http://scholar.utc.edu/cgi/viewcontent.cgi?article=1126& context=theses, (accessed 3 July 2106).

Fruyt, F. and Mervielde, I. (1999) 'RIASEC Types and Big Five Traits as Predictors of Employment Status and Nature of Employment', *Personnel Psychology*, **52**(3), 701-727.

Funicelli, M. (2012) *Personality, Competency and Communicative Suspiciousness Profile of Canadian Police Interrogators of Criminal Suspects*, Concordia University Masters Thesis, available at: http://spectrum.library.concordia.ca/974616/4/ Funicelli_MA_F2012.pdf, (accessed 3 July 2106).

Garaigordobil, M. (2015) ‘Psychometric properties of the Cyberbullying Test, a screening instrument to measure cybervictimization, cyberaggression, and cyberobservation’ *Journal of interpersonal violence*, 0886260515600165.

Garbarino, S., Chiorri, C., Magnavita, N., Piattino, S. and Cuomo, G. (2012) ‘Personality Profiles of Special Force Police Officers’ *Journal of Police and Criminal Psychology*, vol. 27, no. 2, 99-110.

Gartner (2015) *Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015* [press release] available at: http://www.gartner.com/newsroom/id/3165317 (accessed 4 March 2016).

Gilbert, N. (2008) ‘Research, Theory and Method’ in N. Gilbert (ed.) *Researching Social Life* (3rd Edition), London: Sage, 21-40.

Gill, M. ed. (1994) *Crime at Work Vol 1: Studies in Security and Crime Prevention*, Leicester: Perpetuity Press.

Goldberg, L. R. (1981) ‘Language and individual differences: The search for universals in personality lexicons’ in L. Wheeler (ed.), *Review of personality and social psychology*, (Vol. 2, 141- 165). Beverly Hills, CA: Sage.

Goldman, S. (2016) ‘IT Talent Gap an “Existential Threat” in Need of New Tactics’ *CIO*, 11th May, available at: http://www.cio.com/article/3068595/leadership-management/it-talent-gap-an-existential-threat-in-need-of-new-tactics.html, (accessed June 1, 2016).

Guest, G., MacQueen, K. M. and Namey, E. E. (2011) *Applied thematic analysis*, London: Sage.

Halevi, T., Lewis, J., and Memon, N. (2013) ‘A pilot study of cyber security and privacy related behavior and personality traits’ in *Proceedings of the 22nd International Conference on World Wide Web* (737-744). ACM.

Heckman, J. J. and Kautz, T. (2012) ‘Hard evidence on Soft Skills’ *Labour Econ*, **19**(4): 451-464, available at: http://www.nber.org.ezproxy4. lib.le.ac.uk/papers/w18121.pdf, (accessed 6 July 2016).

Hernandez-Castro, J., and Boiten, E. (2014) ‘Cybercrime prevalence and impact in the UK’ *Computer Fraud & Security*, *2014*(2), 5-8.

Hine, C. (2008) ‘The Internet and Research Methods’ in N. Gilbert (ed.) *Researching Social Life* (3rd Edition), London: Sage, 304-320.

Hogan, R. and Kurtines, W. (1975) ‘Personological Correlates of Police Effectiveness’ *The Journal of Psychology*, vol. 91, no. 2, 289-295.

Hollin, C. (2007) ‘Criminological Psychology’ in M. Maguire, R. Morgan, and R. Reiner (eds) *The Oxford Handbook of Criminology* (4th Edition), Oxford: Oxford University Press, 43-77.

Howar, J., Mead, N. and Seshagiri, G. (2016) ‘Using An Apprenticeship Model to Meet Industry Needs for Secure Software Development’ *NICE Newsletter*, available at: http://csrc.nist.gov/nice/enewsletter/eNewsletter_002.html, (accessed 30 August 2016).

Howard, P. J. and Howard, J. M. (1995) ‘The Big Five Quickstart: An Introduction to the Five-Factor Model of Personality for Human Resource Professionals’ *Center for Applied Cognitive Studies*, available at http://files.eric.ed.gov/fulltext/ED384754.pdf, (accessed 6 July 2016).

Intel/CSIS (2016) ‘Hacking the Skill Shortage: A study of the international shortage of cybersecurity skills’ available at https://newsroom.intel.com/news-releases/global-study-reveals-businesses-countries-vulnerable-due-shortage-cybersecurity-talent/ (accessed 30 July 2016)

Interpol (2012) ‘World must better prepare itself for emerging cybercrime threats, INTERPOL Chief tells prestigious meeting in India’ Media release, 30th March, available at http://www.interpol.int/News-and-media/News/2012/PR028, (accessed 3 July 2106).

IPIP (2016) 'International Personality Item Pool: A Scientific Collaboratory for the Development of Advanced Measures of Personality and Other Individual Differences' website, available at: http://ipip.ori.org, (accessed 3 February 2016).

ISACA (2015) '2015 Global Cybersecurity Status Report' *ISACA*, available at: http://www.isaca.org/cyber/Documents/2015-Global-Cybersecurity-Status-Report-Data-Sheet_mkt_Eng_0115.pdf, (accessed 3 July 2106).

ISACA (2016a) *January 2016 Cybersecurity Snapshot*, ISACA, available at: http://www.isaca.org/pages/2016-cybersecurity-snapshot.aspx, (accessed 1 July 2016).

ISACA (2016b) *State of Cybersecurity: Implications for 2016*, ISACA, available at http://www.isaca.org/cyber/Documents/state-of-cybersecurity_res_eng_0316.pdf, (accessed 3 April 2016).

Juniper (2015) *Internet of Things' Connected Devices to Almost Triple to Over 38 Billion Units by 2020* [press release] available at: http://www.isaca.org/cyber/Documents/state-of-cybersecurity_res_eng_0316.pdf http://www.juniperresearch.com/press/press-releases/iot-connected-devices-to-triple-to-38-bn-by-2020, (accessed 15 August 2016).

Klahr, R., Amili, S., Shah, J. N., Button, M. and Wang, V. (2016) *Cyber Security Breaches Survey 2016*, UK Department for Culture, Media & Sport, available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/521465/Cyber_Security_Breaches_Survey_2016_main_report_FINAL.pdf, (accessed 2 August 2106).

Koops, B. (2011) The Internet and its Opportunities for Cybercrime, Tilburg Law School Legal Studies Research Paper Series, No. 9/2011.

Langner, R. (2011) 'Stuxnet: Dissecting a cyberwarfare weapon' *IEEE Security & Privacy*, *9*(3), 49-51.

Lemos, R. (2016) 'IT Security Skills Gap More Harmful for SMBs Than Larger Firms' *eWeek*, 3rd July, available at: http://www.eweek.com/security/it-security-skills-gap-more-harmful-for-smbs-than-larger-firms.html, (accessed 14 July 2106).

Libicki, M. C., Senty, D., and Pollak, J. (2014) *Hackers Wanted: an examination of the cybersecurity labor market*. Rand Corporation, available at: http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR430/RAND_RR430.pdf, (accessed 3 July 2106).

Maio, P. (2016) 'New computer science course's challenge is finding qualified teachers to teach it' *EdSource*, 23rd August, available at: https://edsource.org/2016/new-computer-science-courses-challenge-is-finding-qualified-teachers-to-teach-it/568081, (access August 29, 2016).

Marshall, P. (2015) 'The sharing economy' *SAGE Business Researcher*, 3rd August Retrieved from http://businessresearcher.sagepub.com, (accessed 3 May 2106).

McCrae, R. R. and Costa, P. T. (1987) 'Validation of the five-factor model of personality across instruments and observers' *Journal of personality and social psychology*, **52**(1), 81.

McDonald, S. and Edwards, H. M. (2007) 'Who should test whom?' *Communications of the ACM*, 50(1), 66-71.

McNeeley, S. (2015) 'Lifestyle-Routine Activities and Crime Events' *Journal of Contemporary Criminal Justice,* **31**(1), 30-52.

Megaw, N. (2015) 'Cyber security sector struggles to fill skills gap' *FT*, 18th November 18, available at: http://www.ft.com/cms/s/0/4cabd0fe-8940-11e5-90de-f44762bf9896.html#axzz4Irh0vW3o (accessed 27 February 2016).

Metzger, M. (2016) 'Cyber-crime now included in government crime stats' *SC Magazine*, 21st July, available at: http://www.scmagazineuk.com/cyber-crime-now-included-in-government-crime-stats/article/510937, (accessed 24 July 2016).

Modic, D., and Lea, S. E. G. (2012) 'How neurotic are scam victims, really? The big five and Internet scams' Paper presented at the *2011 Conference of the International Confederation for the Advancement of Behavioral Economics and Economic Psychology*, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id= 2448130, accessed 23 August 2016).

Morgan, S. (2016) 'One Million Cybersecurity Job Openings In 2016' *Forbes*, January 2, available at: http://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/#1ed106a77d27, (accessed 13 March 2106).

Morris, J. and Waage, E. (2015) 'Cyber Aptitude Assessment: Finding the Next Generation of Enlisted Cyber Soldiers' *The Cyber Defense Review*, November 16, available at: http://www.cyberdefensereview.org/2015/11/16/cyber-aptitude, (accessed 3 July 2106).

Muck, P.M., Hell, B., and Gosling, S.D. (2007) 'Construct validation of a short five-factor model instrument: A self-peer study on the German adaptation of the Ten-Item Personality Inventory (TIPI-G)' *European Journal of Psychological Assessment*, 23, 166–175.

Neuman, G.A. and Wright, J. (1999) 'Team Effectiveness: Beyond Skills and Cognitive Ability', *Journal of Applied Psychology,* **84**(3), 376-389.

Newman, G.R. and Clarke, R.V.G. (2003) Superhighway robbery: preventing e-commerce crime, Cullompton: Willan.

NICCS (2016) 'National Initiative for Cybersecurity Careers and Studies' website, https://niccs.us-cert.gov, (accessed 1 July, 2016)

NICE (2014) *National Cybersecurity Workforce Framework*, website and link to the interactive version, available at: http://csrc.nist.gov/nice/framework, (accessed 3 July 2106).

NIST (2014) *Cybersecurity Framework* NIST website, available at: http://www.nist.gov/cyberframework/ and NIST Framework document available at: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf, (accessed 21 July 2016).

O'Neill, M. (2011) *What makes a successful volume crime investigator?* Doctoral dissertation, University of Portsmouth, available at http://eprints.port.ac.uk/8517/1/Martins_PHD.pdf, (accessed 3 July 2106).

O'Neil, L. R., Greitzer, F. L., Conway, T. J., Dalton, A. C., Tobey, D. H., and Pusey, P. K. (2014). 'Secure Power Systems Professional Phase III Final Report: Recruiting, Selecting and Developing Secure Power Systems Professionals' available at: https://www.controlsystemsroadmap.net/ieRoadmap%20Documents/SPSP_Phase3.pdf, (accessed 13 June 2106).

O*NET (2016) 'Summary Report for: 15-1122.00 - Information Security Analysts' O*NET OnLine, available at: http://www.onetonline.org/link/summary/15-1122.00, (accessed 15 July 2016).

Oberoi, M. (2016) National Capacity Strengthening to Combat Cybercrime CYFY July 21, 2016 http://cyfy.org/national-capacity-strengthening-to-combat-cybercrime, (accessed 31 July 2016).

Oltsik, J. (2016) 'High-demand cybersecurity skill sets' *Network World*, May 10, available at: http://www.networkworld.com/article/3068177/security/high-demand-cybersecurity-skill-sets.html, (accessed 25 July 2016).

Ono, M., Sachau, D. A., Deal, W. P., Englert, D. R., and Taylor, M. D. (2011) 'Cognitive ability, emotional intelligence, and the big five personality dimensions as predictors of criminal investigator performance' *Criminal Justice and Behavior*, 38(5), 471-491.

ONS (2016) Statistical bulletin: Crime in England and Wales: year ending Mar 2016, *Office of National Statistics*, available at https://www.ons.gov.uk/ peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmar2016#statisticians-quote, (accessed 25 July 2016).

OPM (2016) 'CyberCorps: Scholarship For Service' website, available at: https://www.sfs.opm.gov (accessed September 1, 2016).

Owen, S. and Sawhill, I. (2013) 'Should Everyone Go To College?' Brookings Institute, 8th May, available at: https://www.brookings.edu/research/should-everyone-go-to-college, (accessed 27 August 2016).

Peachey, P. (2014) 'Police failing to train key staff to fight growing threat of cyber crime' The Independent, 7th December, available at http://www.independent.co.uk/news/uk/crime/police-failing-to-train-key-staff-to-fight-growing-threat-of-cyber-crime-9909334.html, (accessed 5 March 2016).

Pease, K. (2005) 'Science in the service of crime reduction', in N. Tilley (ed.), *Handbook of Crime Prevention and Community Safety*, Collumpton, Willan Publishing: 39-70.

Peters, S. (2016) 'New White House Cybersecurity Plan Creates Federal CISO' *Dark Reading*, February 9, available at: http://www.darkreading.com/risk/new-white-house-cybersecurity-plan-creates-federal-ciso---/d/d-id/1324243, (accessed 24 March 2016).

Peterson, A. (2016) 'Universities aren't doing enough to train the cyberdefenders America desperately needs' *Washington Post*, available at https://www.washingtonpost.com/news/the-switch/wp/2016/04/11/universities-arent-doing-enough-to-train-the-cyberdefenders-america-desperately-needs, (accessed 5 May 2016).

Pettigrew, J., and Ryan, J. (2012). Making Successful Security Decisions: A Qualitative Evaluation. *IEEE Security & Privacy*, *1*(10), 60-68.

Platt, J. R. (2015) 'No Clear Path for Prospective Cybersecurity Specialists' *The Institute*, 6th March, available at http://theinstitute.ieee.org/career-and-education/career-guidance/no-clear-path-for-prospective-cybersecurity-specialists (accessed 3 August 2016).

PNNL (2012) *Smart Grid Cybersecurity: Job Performance Model Report* available at: http://energy.gov/sites/prod/files/2013/05/f0/SGC-Report.pdf, (accessed 3 July 2106).

Ponemon (2015) *2015 Cost of Cyber Crime Study: Global*, Ponemon Institute, available at: http://www.cnmeonline.com/myresources/hpe/docs/HPE_SIEM_Analyst_ Report_-_2015_Cost_of_Cyber_Crime_Study_-_Global.pdf, (accessed 4 July 2016).

Potter, L. E., and Vickers, G. (2015) 'What Skills do you Need to Work in Cyber Security?: A Look at the Australian Market' in P*roceedings of the 2015 ACM SIGMIS Conference on Computers and People Research* ACM, 67-72.

PPS (2009) *Cyber IN-SECURITY: Strengthening the Federal Cybersecurity Workforce*, Partnership for Public Service and Booz Allen Hamilton, available at: https://www.boozallen.com/content/dam/boozallen/media/file/CyberIn-Security_2009.pdf, (accessed 25 May 2016).

Rafter, N.H. (2006) 'H. J. Eysenck in Fagin's kitchen: the return to biological theory in 20th-century criminology', *History of the Human Sciences,* **19**(4), 37-56.

Real Clear Politics (2009) 'Secretary Gates Talks to Troops in Alabama' *Real Clear Politics,* 15th April, available at: http://www.realclearpolitics.com/articles/2009/04/15/ gates_talks_to_troops_in_alabama_96023.html#ixzz4DNvqTeHg, (accessed 25 May 2106).

Ree, M.J., Earles, J.A. and Teachout, M.S. (1994) 'Predicting Job Performance: Not Much More Than g' *Journal of Applied Psychology*, vol. 79, no. 4, 518-524.

Riek, M., Böhme, R., and Moore, T. (2016). Measuring the influence of perceived cybercrime risk on online service avoidance. *IEEE Transactions on Dependable and Secure Computing*, *13*(2), 261-273.

Ring, T. (2014) 'Police need more money to fight cyber-crime, finds report' *SC Magazine UK*, 9th December, available at: http://www.scmagazineuk.com/police-need-more-money-to-fight-cyber-crime-finds-report/article/387315, (accessed 11 May 2106).

Robertson, J. and Riley, M. (2015) 'JPMorgan Reassigns Security Team Leader a Year After Data Breach' *Bloomberg*, 30th June, available at: http://www.bloomberg.com/news/articles/2015-06-30/jpmorgan-reassigns-security-team-leader-a-year-after-data-breach, (accessed 5 May 2106).

Ryan, J. and Jefferson, T. (2003) 'The Use, Misuse and Abuse of Statistics in Information Security Research' *Proceedings of the 23rd ASEM National Conference*, ASEM 15-18 October 2003.

Saldana, J. (2013) *The Coding Manual for Qualitative Researchers* (2nd Edition), Sage: London.

Sanders, B.A. (2008) 'Using personality traits to predict police officer performance' *Policing: An International Journal of Police Strategies & Management,* vol. 31, no. 1, 129-147.

Satelvad, A. (2015) 'Demand to fill cybersecurity jobs booming' *Peninsula Press*, 31st March, available at: http://peninsulapress.com/2015/03/31/cybersecurity-jobs-growth, (accessed 15 June 2106).

Schmidt, F. L. (2002) 'The role of general cognitive ability and job performance: Why there cannot be a debate' *Human performance*, 15(1-2), 187-210.

SEC (2015) 'The Need for Greater Focus on the Cybersecurity Challenges Facing Small and Midsize Businesses' Public statement of U.S. Securities and Exchange Commission, 19th October, available at: https://www.sec.gov/news/statement/ cybersecurity-challenges-for-small-midsize-businesses.html#_edn6, (accessed 23 August 2015).

Seglins, D. and Burgess, L. (2015) 'Canada 'failing' in fight against cybercrime, hacking' *CBC*, 11th November, available at: http://www.cbc.ca/news/technology/canada-cybercrime-hacking-seglins-1.3312153, (accessed 15 May 2106).

Simpson, D. (2005). Phrenology and the neurosciences: contributions of FJ Gall and JG Spurzheim. *ANZ journal of surgery*, *75*(6), 475-482.

Smith, G.S. (2015) 'Management models for international cybercrime' *Journal of Financial Crime*, **22**(1): 104-125.

Smith, N., Flanagan, C. and Great Britain. Home Office.Policing and Reducing Crime Unit (2000) *The effective detective: identifying the skills of an effective SIO.* London: Home Office.

Sorebo, G. (2014) 'The Cybersecurity Skills Gap: A Real or Manufactured Crisis?' *RSA Conference*, 5th May, available at: http://www.rsaconference.com/blogs/the-cybersecurity-skills-gap-a-real-or-manufactured-crisis#sthash.hGtWCjcA.dpuf, (accessed 17 May 2106).

Spearman, C. (1904) '"General Intelligence," Objectively Determined and Measured' *The American Journal of Psychology*, Vol. 15, No. 2 (Apr., 1904), 201-292, available at: http://www.jstor.org/stable/1412107, (accessed 15 May 2106).

Staude-Müller, F., Hansen, B., and Voss, M. (2012). How stressful is online victimization? Effects of victim's personality and properties of the incident. *European Journal of Developmental Psychology*, **9**(2), 260-274.

Staw, B. M. (1986) 'Organizational psychology and the pursuit of the happy/productive worker' *California Management Review*, **28**(4), 40-53.

Sturgis, (2008) 'Designing Samples' in N. Gilbert (ed.) *Researching Social Life* (3rd Edition), London: Sage, 304-320.165-181

Symonds, William C., Robert Schwartz, and Ronald F. Ferguson (2011) 'Pathways to prosperity: Meeting the challenge of preparing young Americans for the 21st century' Pathways to Prosperity Project, Harvard University Graduate School of Education, available at http://nrs.harvard.edu/urn-3:HUL.InstRepos:4740480, (accessed 15 July 2016).

Taber, J. (1980) A Survey of Computer Crime Studies 2 *Computer Law Journal*, 275 (1980) available at: http://repository.jmls.edu/jitpl/vol2/iss1/15 (accessed 23 February 2016).

Tobey, D. (2015) 'A Vignette-based Method for Improving Cybersecurity Talent Management through Cyber Defense Competition Design' in *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research*, ACM: 31-39.

Tobey, D. H., Pusey, P. and Burley, D. L. (2014) ‘Engaging learners in cybersecurity careers: lessons from the launch of the national cyber league’ *ACM Inroads*, *5*(1), 53-56.

Townsend, K. (2016) ‘Recruitment Challenges Continue to Plague Cyber Security’ *Security Week*, 11th April, available at http://www.securityweek.com/recruitment-challenges-continue-plague-cyber-security, (accessed 1 August 2016).

Turgeon, W. (2016) ‘The IT skills shortage — fact or myth?’ *IT World Canada*, 8th March, available at: http://www.itworldcanada.com/blog/the-it-skills-shortage-fact-or-myth/381501#ixzz4Dx4NsFVl, (accessed 15 June 2106).

USAF (2005) ‘Cyberspace as a Domain In which the Air Force Flies and Fights: Remarks as delivered to the C4ISR Integration Conference, Nov. 2, 2006’ *U.S. Air Force website,* available at: http://www.af.mil/AboutUs/SpeechesArchive/Display/tabid/268/Article/143968/cyberspace-as-a-domain-in-which-the-air-force-flies-and-fights.aspx, (accessed 15 June 2106).

USAF (2009) ‘The Cyber Menace’ *AIR FORCE Magazine*, March, available at: http://www.airforcemag.com/magazinearchive/documents/2009/march%202009/0309cyber.pdf, (accessed 15 June 2106).

Varela, J. G., Boccaccini, M. T., Scogin, F., Stump, J., & Caputo, A. (2004). Personality testing in law enforcement employment settings: A meta-analytic review. *Criminal Justice and Behavior*, *31*, 649-675.

Wajsgras, D. (2016) ‘The Time Is Now to Prevent a Cybersecurity Workforce Crisis’ *US News*, 8th June, available at: http://www.usnews.com/news/articles/2016-06-08/op-ed-the-time-is-now-to-prevent-a-cybersecurity-workforce-crisis, (accessed 15 June 2106).

Wall, D. S. (2008) ‘Cybercrime and the Culture of Fear: Social Science Fiction(s) and the Production of Knowledge about Cybercrime (Revised Feb. 2011)’ *Information, Communication & Society,* Vol. 11, No. 6: 861-884.

Westera, N.J., Kebbell, M.R., Milne, B. and Green, T. (2014) 'Towards a more effective detective' *Policing and Society,* **26**(1), 1-17.

Westmarland, L. (2011) *Researching crime and justice: tales from the field.* London: Routledge.

Whalen, T. and Gates, C. (2007) ‘A psychological profile of defender personality traits’ *Journal of Computers*, 2(2), 84-93.

White House (1997) *President’s Commission on Critical Infrastructure Protection, Critical Foundations: Protecting America’s infrastructures*, available at: http://www.fas.org/sgp/library/pccip.pdf, (accessed 15 June 2106).

White House (2016) *FACT SHEET: Cybersecurity National Action Plan*, available at: https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan, (accessed 15 June 2106).

Wikström, P. O. H. (1995). Preventing city-center street crimes. *Crime and justice*, in

Wood, S. (2006) ‘New Air Force Command to Fight in Cyberspace’ *American Forces Press Service*, accessed ahttp://archive.defense.gov/news/newsarticle.aspx?id=2014

Wright, T. A., and Cropanzano, R. (2004) ‘The Role of Psychological Well-Being in Job Performance:: A Fresh Look at an Age-Old Quest’ *Organizational Dynamics*, **33**(4), 338-351.

Yadron, D. (2014) ‘Police Grapple With Cybercrime’ *WSJ* 20th April, available at http://www.wsj.com/articles/SB10001424052702304626304579508212978109316, (accessed 15 June 2106).

Yoakum, C. S., and Yerkes, R. M. (1920) *Army mental tests*, New York: H. Holt.

Appendices

Appendix A: Ethics approval

University Ethics Sub-Committee for Sociology;
Politics and IR; Lifelong Learning;
Criminology; Economics and the
School of Education

09/06/2016

Ethics Reference: 6425-stc16-criminology

TO:
Name of Researcher Applicant: Stephen Cobb
Department: Criminology
Research Project Title: Characteristics of effective chief information security officers
Module Name or Course: Dissertation CR7521 MSc Security and Risk Management, Department of Criminology
Supervisor's or Module Leader's Name: Mark Connor

Dear Stephen Cobb,

RE: Ethics review of Research Study application

The University Ethics Sub-Committee for Sociology; Politics and IR; Lifelong Learning; Criminology; Economics and the School of Education has reviewed and discussed the above application.

1. Ethical opinion

The Sub-Committee grants ethical approval to the above research project on the basis described in the application form and supporting documentation, subject to the conditions specified below.

2. Summary of ethics review discussion

The Committee noted the following issues:
Your application has been approved please retain this conformation, forward to your supervisor and include a copy in the appendix of your final dissertation. Any significant change to the methodology or sample indicated in this application must be discussed with your supervisor and may be subject to further ethical review.

3. General conditions of the ethical approval

The ethics approval is subject to the following general conditions being met prior to the start of the project:

As the Principal Investigator, you are expected to deliver the research project in accordance with the University's policies and procedures, which includes the University's Research Code of Conduct and the University's Research Ethics Policy.

If relevant, management permission or approval (gate keeper role) must be obtained from host organisation prior to the start of the study at the site concerned.

4. Reporting requirements after ethical approval

You are expected to notify the Sub-Committee about:

- Significant amendments to the project
- Serious breaches of the protocol
- Annual progress reports
- Notifying the end of the study

5. Use of application information

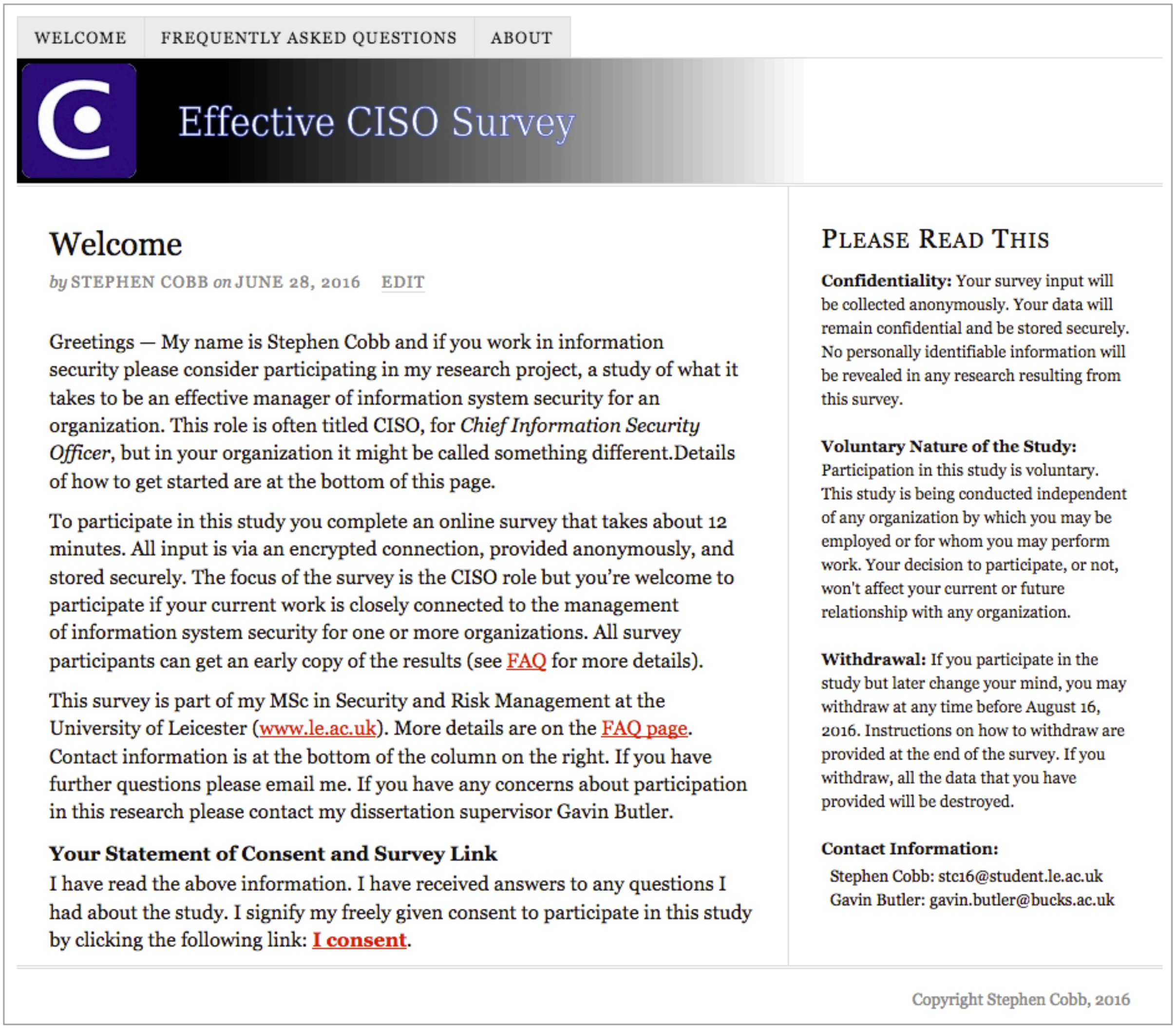
Details from your ethics application will be stored on the University Ethics Online System. With your permission, the Sub-Committee may wish to use parts of the application in an anonymised format for training or sharing best practice. Please let me know if you do not want the application details to be used in this manner.

Best wishes for the success of this research project.

Yours sincerely,

Dr. Laura Brace
Chair

Appendix B: The CISO Survey web portal



Effective CISO Survey

Welcome

by STEPHEN COBB *on* JUNE 28, 2016 EDIT

Greetings — My name is Stephen Cobb and if you work in information security please consider participating in my research project, a study of what it takes to be an effective manager of information system security for an organization. This role is often titled CISO, for *Chief Information Security Officer*, but in your organization it might be called something different.Details of how to get started are at the bottom of this page.

To participate in this study you complete an online survey that takes about 12 minutes. All input is via an encrypted connection, provided anonymously, and stored securely. The focus of the survey is the CISO role but you're welcome to participate if your current work is closely connected to the management of information system security for one or more organizations. All survey participants can get an early copy of the results (see FAQ for more details).

This survey is part of my MSc in Security and Risk Management at the University of Leicester (www.le.ac.uk). More details are on the FAQ page. Contact information is at the bottom of the column on the right. If you have further questions please email me. If you have any concerns about participation in this research please contact my dissertation supervisor Gavin Butler.

Your Statement of Consent and Survey Link

I have read the above information. I have received answers to any questions I had about the study. I signify my freely given consent to participate in this study by clicking the following link: **I consent**.

Please Read This

Confidentiality: Your survey input will be collected anonymously. Your data will remain confidential and be stored securely. No personally identifiable information will be revealed in any research resulting from this survey.

Voluntary Nature of the Study: Participation in this study is voluntary. This study is being conducted independent of any organization by which you may be employed or for whom you may perform work. Your decision to participate, or not, won't affect your current or future relationship with any organization.

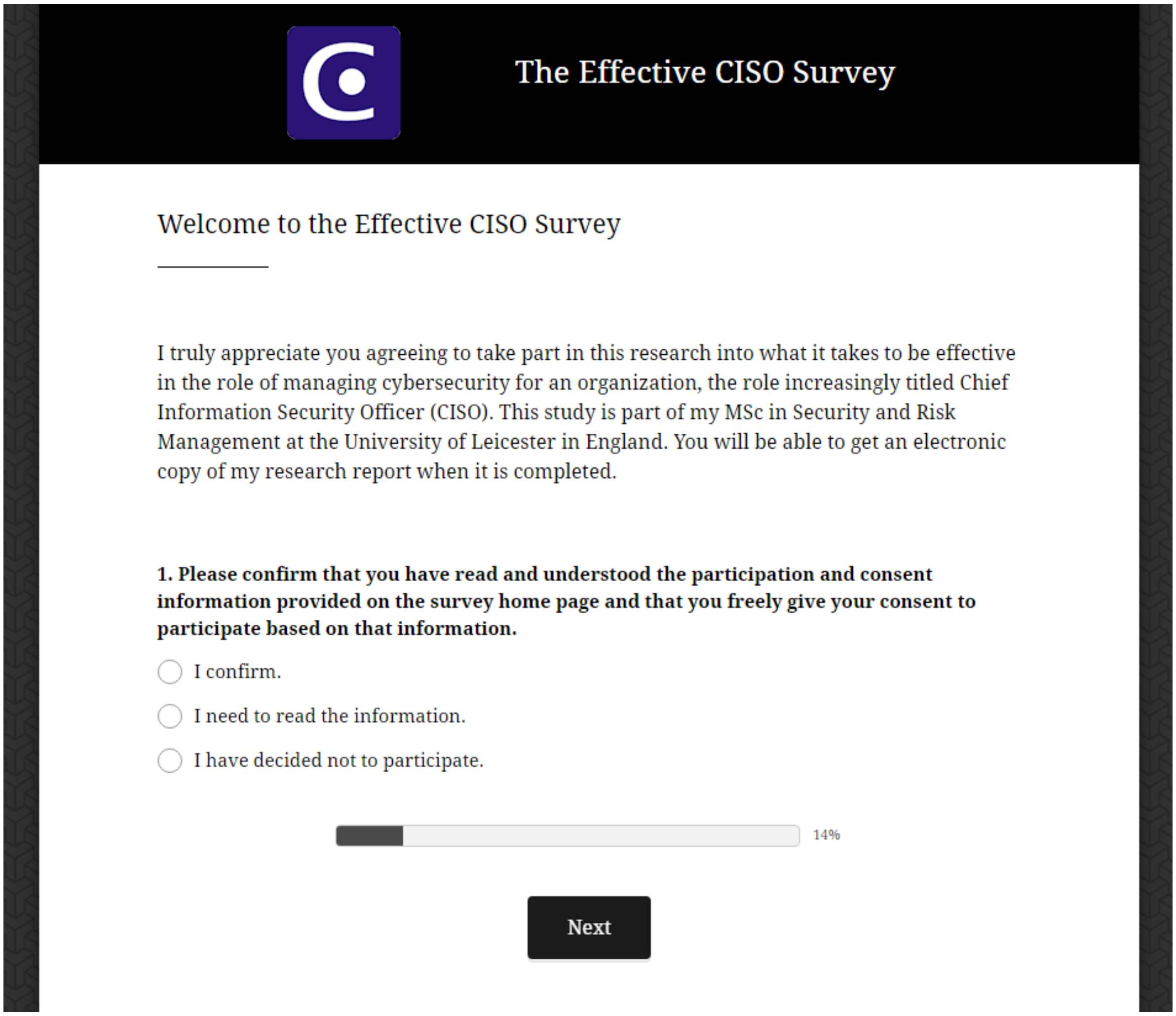
Withdrawal: If you participate in the study but later change your mind, you may withdraw at any time before August 16, 2016. Instructions on how to withdraw are provided at the end of the survey. If you withdraw, all the data that you have provided will be destroyed.

Contact Information:

Stephen Cobb: stc16@student.le.ac.uk
Gavin Butler: gavin.butler@bucks.ac.uk

Copyright Stephen Cobb, 2016

Appendix C: The CISO Survey



The Effective CISO Survey

Welcome to the Effective CISO Survey

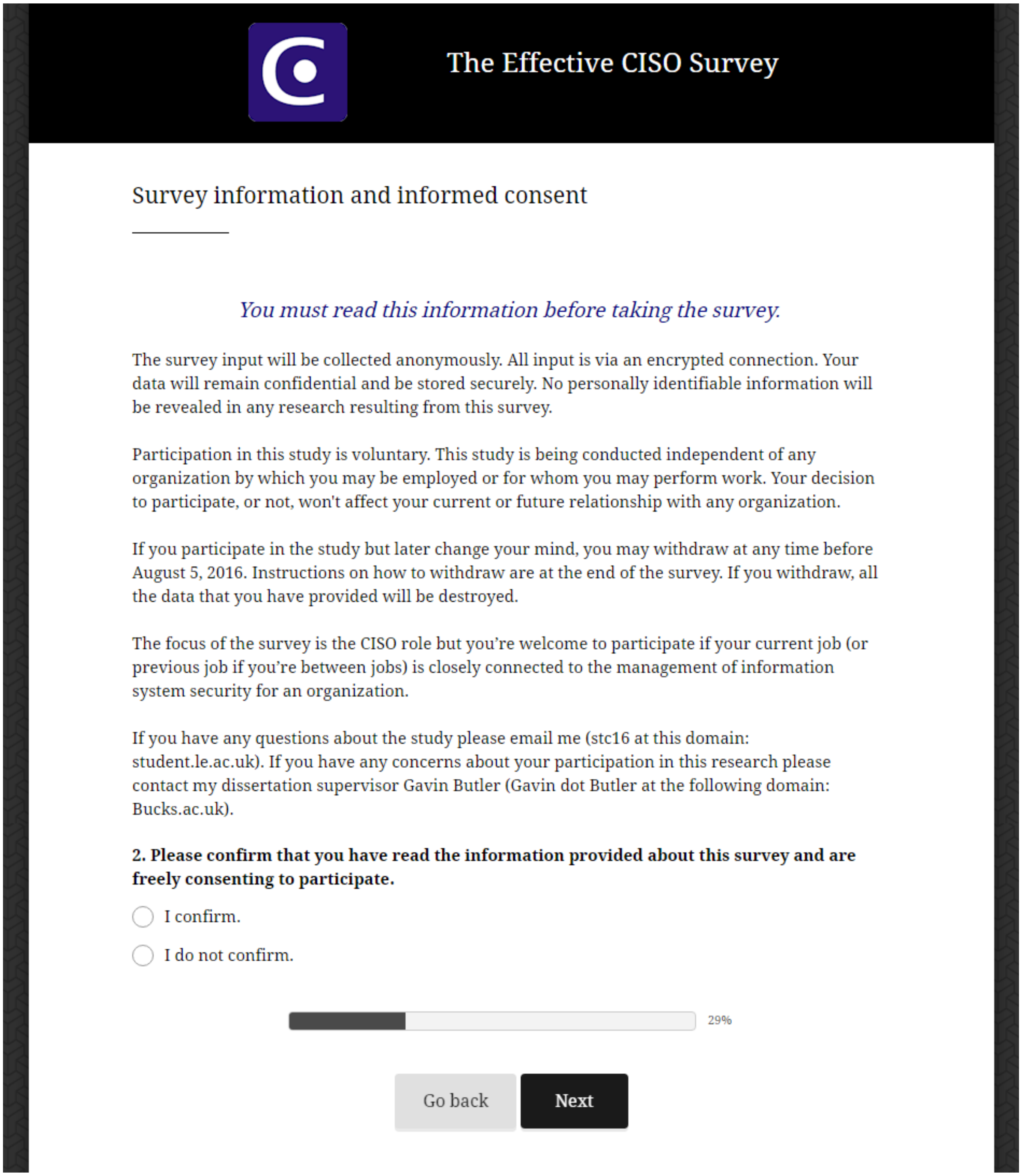
I truly appreciate you agreeing to take part in this research into what it takes to be effective in the role of managing cybersecurity for an organization, the role increasingly titled Chief Information Security Officer (CISO). This study is part of my MSc in Security and Risk Management at the University of Leicester in England. You will be able to get an electronic copy of my research report when it is completed.

1. Please confirm that you have read and understood the participation and consent information provided on the survey home page and that you freely give your consent to participate based on that information.

○ I confirm.

○ I need to read the information.

○ I have decided not to participate.



Survey information and informed consent

You must read this information before taking the survey.

The survey input will be collected anonymously. All input is via an encrypted connection. Your data will remain confidential and be stored securely. No personally identifiable information will be revealed in any research resulting from this survey.

Participation in this study is voluntary. This study is being conducted independent of any organization by which you may be employed or for whom you may perform work. Your decision to participate, or not, won't affect your current or future relationship with any organization.

If you participate in the study but later change your mind, you may withdraw at any time before August 5, 2016. Instructions on how to withdraw are at the end of the survey. If you withdraw, all the data that you have provided will be destroyed.

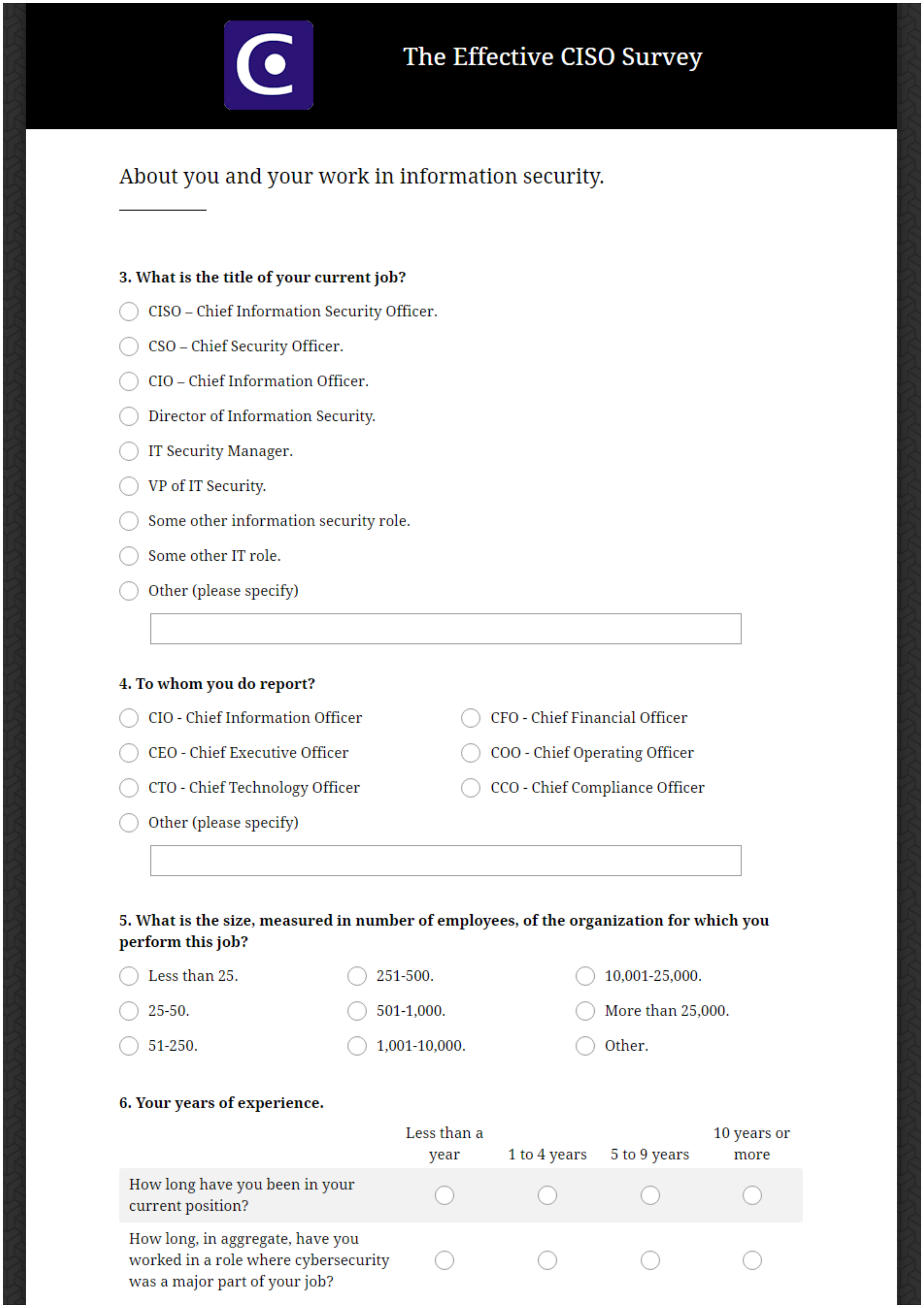
The focus of the survey is the CISO role but you're welcome to participate if your current job (or previous job if you're between jobs) is closely connected to the management of information system security for an organization.

If you have any questions about the study please email me (stc16 at this domain: student.le.ac.uk). If you have any concerns about your participation in this research please contact my dissertation supervisor Gavin Butler (Gavin dot Butler at the following domain: Bucks.ac.uk).

2. Please confirm that you have read the information provided about this survey and are freely consenting to participate.

○ I confirm.

○ I do not confirm.



The Effective CISO Survey

About you and your work in information security.

3. What is the title of your current job?

○ CISO – Chief Information Security Officer.

○ CSO – Chief Security Officer.

○ CIO – Chief Information Officer.

○ Director of Information Security.

○ IT Security Manager.

○ VP of IT Security.

○ Some other information security role.

○ Some other IT role.

○ Other (please specify)

4. To whom you do report?

○ CIO - Chief Information Officer

○ CEO - Chief Executive Officer

○ CTO - Chief Technology Officer

○ CFO - Chief Financial Officer

○ COO - Chief Operating Officer

○ CCO - Chief Compliance Officer

○ Other (please specify)

5. What is the size, measured in number of employees, of the organization for which you perform this job?

○ Less than 25.

○ 25-50.

○ 51-250.

○ 251-500.

○ 501-1,000.

○ 1,001-10,000.

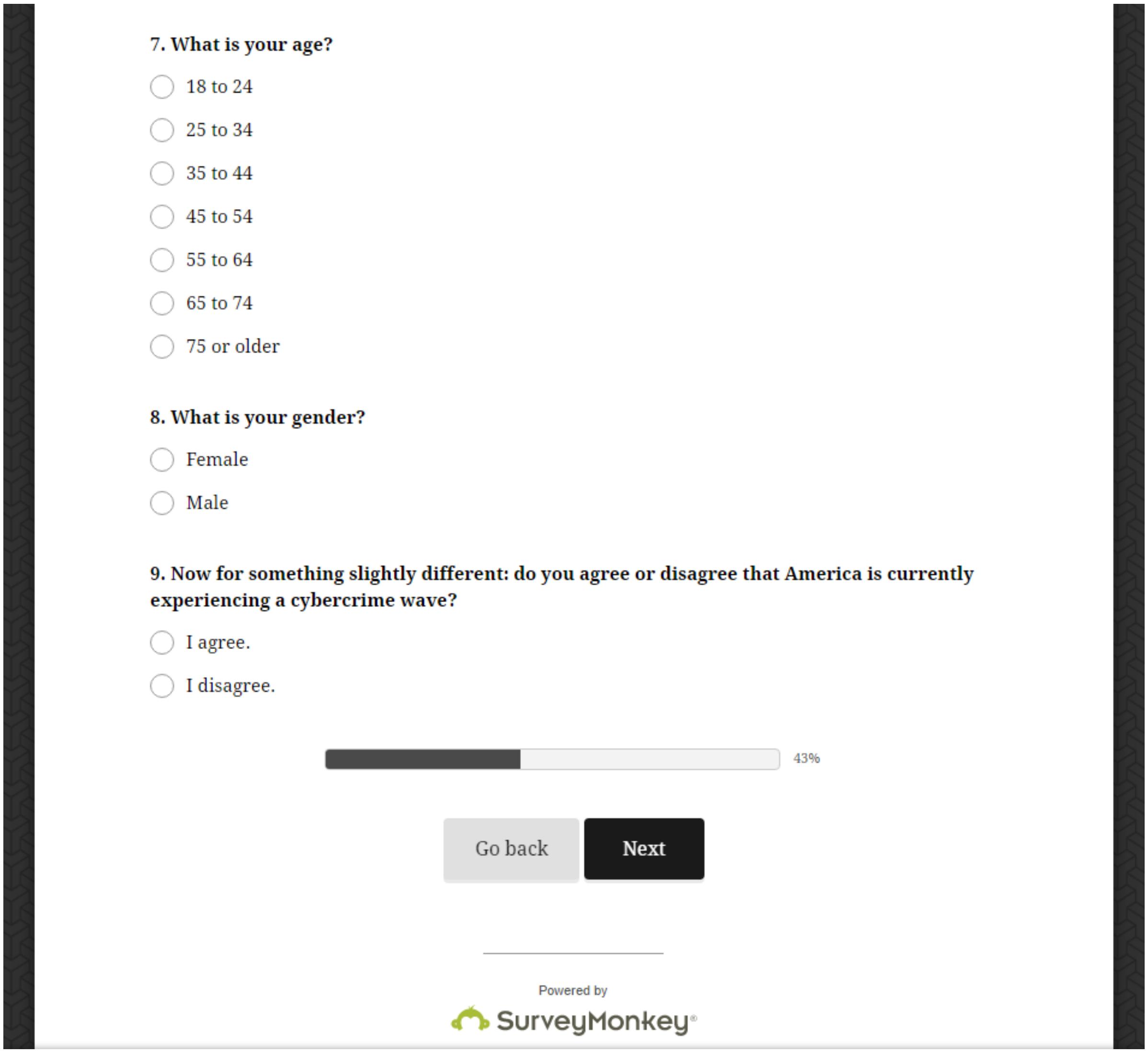
○ 10,001-25,000.

○ More than 25,000.

○ Other.

6. Your years of experience.

	Less than a year	1 to 4 years	5 to 9 years	10 years or more
How long have you been in your current position?	○	○	○	○
How long, in aggregate, have you worked in a role where cybersecurity was a major part of your job?	○	○	○	○



7. What is your age?

○ 18 to 24

○ 25 to 34

○ 35 to 44

○ 45 to 54

○ 55 to 64

○ 65 to 74

○ 75 or older

8. What is your gender?

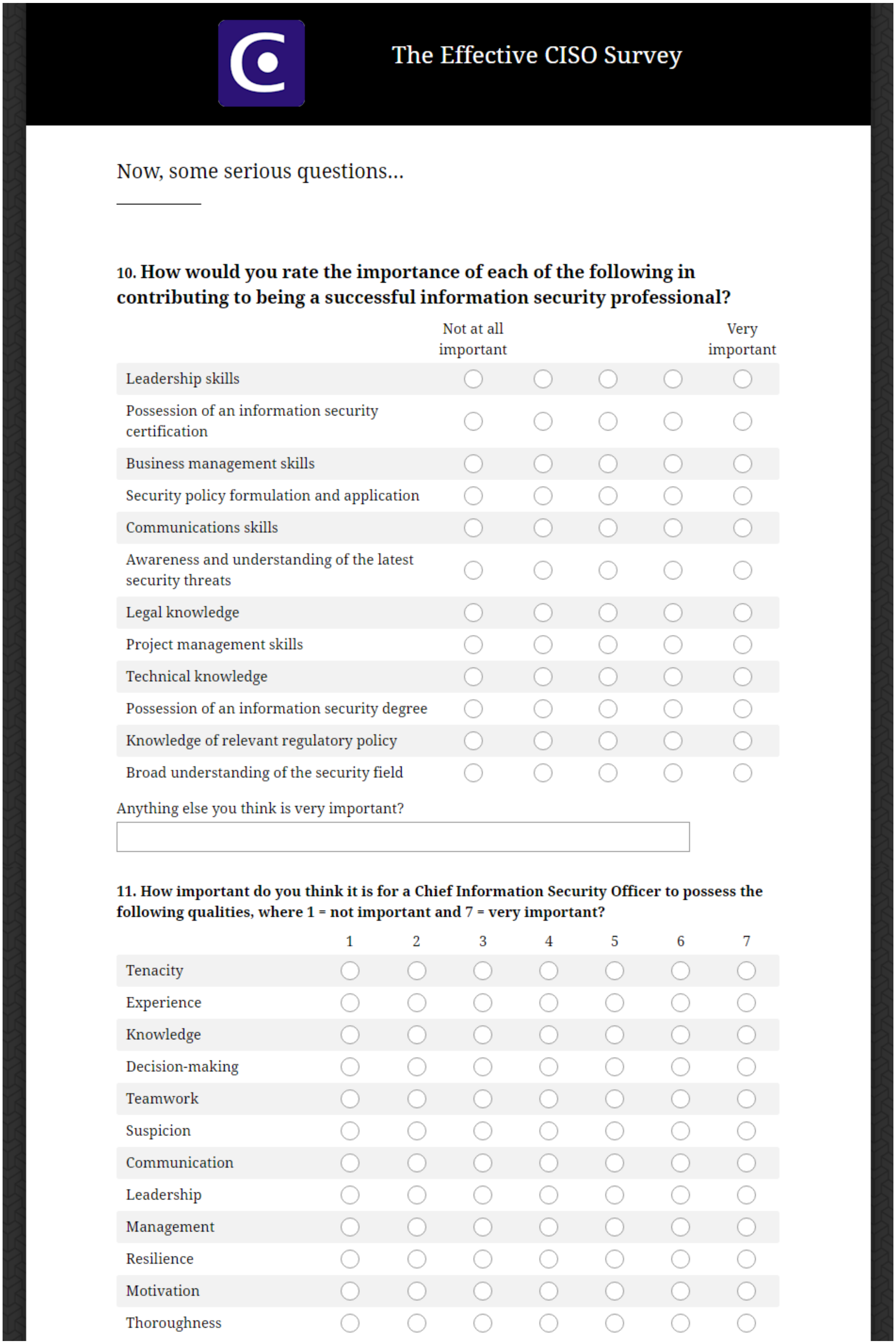
○ Female

○ Male

9. Now for something slightly different: do you agree or disagree that America is currently experiencing a cybercrime wave?

○ I agree.

○ I disagree.



The Effective CISO Survey

Now, some serious questions...

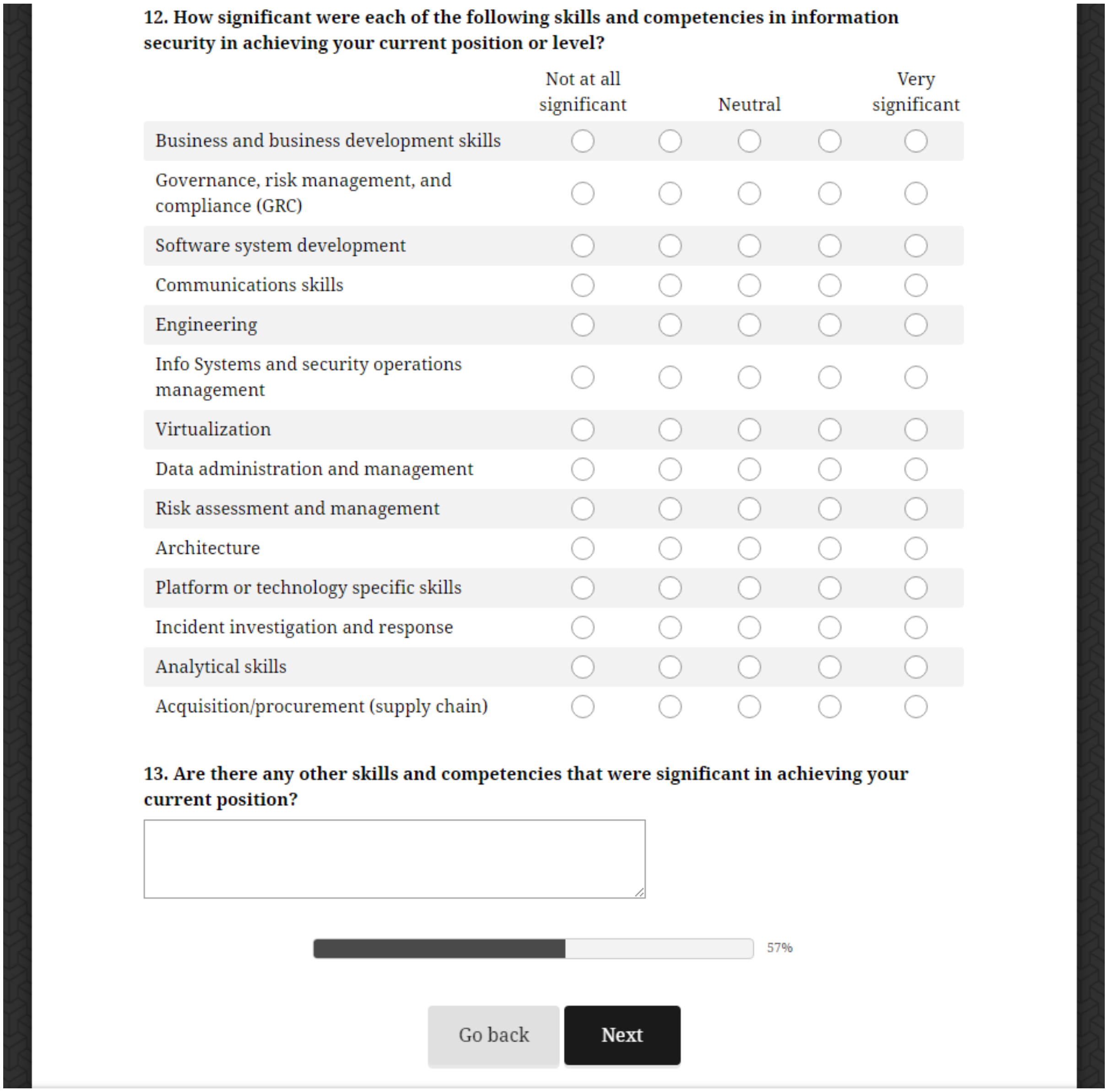
10. How would you rate the importance of each of the following in contributing to being a successful information security professional?

	Not at all important				Very important
Leadership skills	○	○	○	○	○
Possession of an information security certification	○	○	○	○	○
Business management skills	○	○	○	○	○
Security policy formulation and application	○	○	○	○	○
Communications skills	○	○	○	○	○
Awareness and understanding of the latest security threats	○	○	○	○	○
Legal knowledge	○	○	○	○	○
Project management skills	○	○	○	○	○
Technical knowledge	○	○	○	○	○
Possession of an information security degree	○	○	○	○	○
Knowledge of relevant regulatory policy	○	○	○	○	○
Broad understanding of the security field	○	○	○	○	○

Anything else you think is very important?

11. How important do you think it is for a Chief Information Security Officer to possess the following qualities, where 1 = not important and 7 = very important?

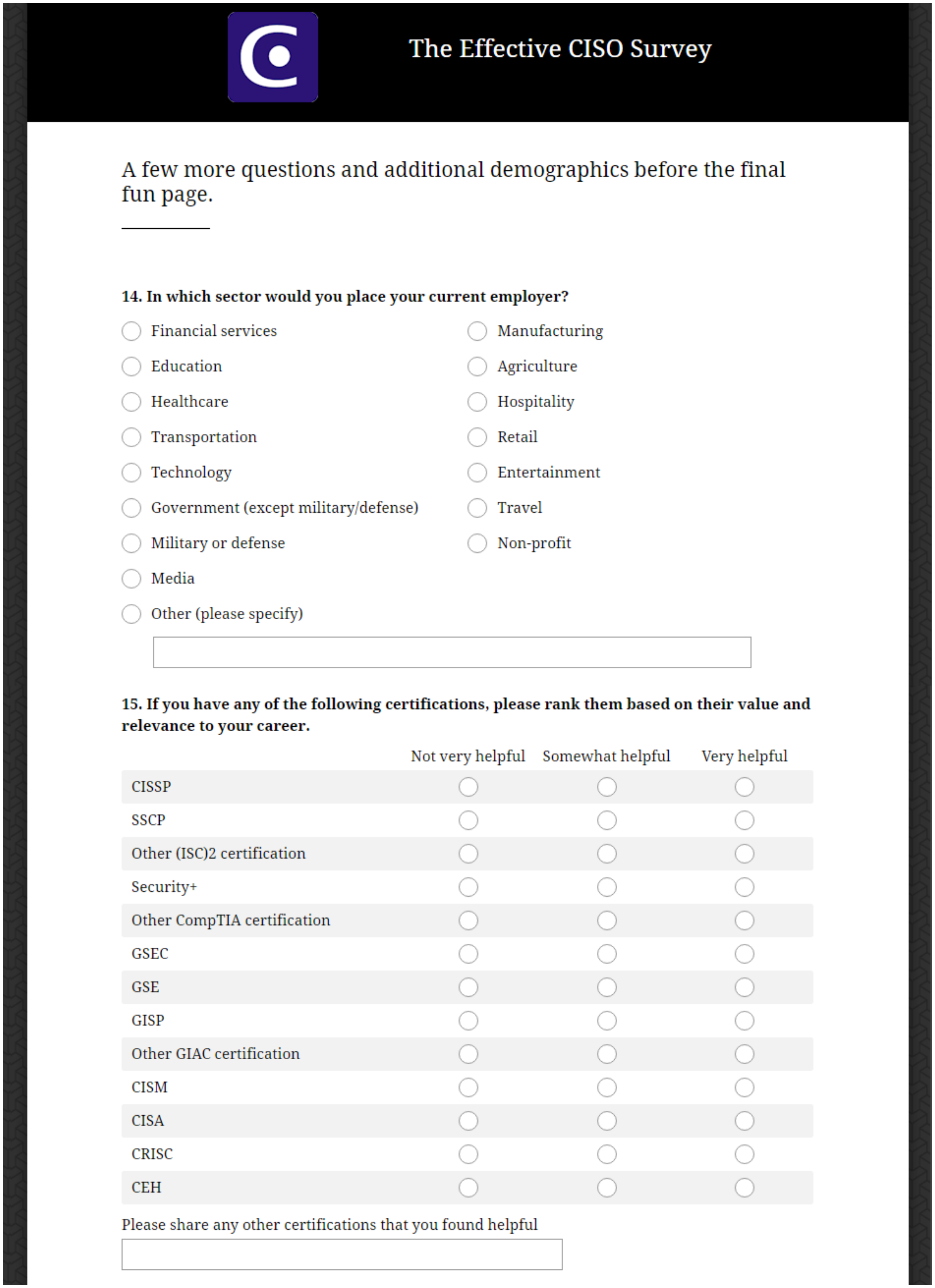
	1	2	3	4	5	6	7
Tenacity	○	○	○	○	○	○	○
Experience	○	○	○	○	○	○	○
Knowledge	○	○	○	○	○	○	○
Decision-making	○	○	○	○	○	○	○
Teamwork	○	○	○	○	○	○	○
Suspicion	○	○	○	○	○	○	○
Communication	○	○	○	○	○	○	○
Leadership	○	○	○	○	○	○	○
Management	○	○	○	○	○	○	○
Resilience	○	○	○	○	○	○	○
Motivation	○	○	○	○	○	○	○
Thoroughness	○	○	○	○	○	○	○



12. How significant were each of the following skills and competencies in information security in achieving your current position or level?

	Not at all significant		Neutral		Very significant
Business and business development skills	○	○	○	○	○
Governance, risk management, and compliance (GRC)	○	○	○	○	○
Software system development	○	○	○	○	○
Communications skills	○	○	○	○	○
Engineering	○	○	○	○	○
Info Systems and security operations management	○	○	○	○	○
Virtualization	○	○	○	○	○
Data administration and management	○	○	○	○	○
Risk assessment and management	○	○	○	○	○
Architecture	○	○	○	○	○
Platform or technology specific skills	○	○	○	○	○
Incident investigation and response	○	○	○	○	○
Analytical skills	○	○	○	○	○
Acquisition/procurement (supply chain)	○	○	○	○	○

13. Are there any other skills and competencies that were significant in achieving your current position?



The Effective CISO Survey

A few more questions and additional demographics before the final fun page.

14. In which sector would you place your current employer?

○ Financial services

○ Education

○ Healthcare

○ Transportation

○ Technology

○ Government (except military/defense)

○ Military or defense

○ Media

○ Other (please specify)

○ Manufacturing

○ Agriculture

○ Hospitality

○ Retail

○ Entertainment

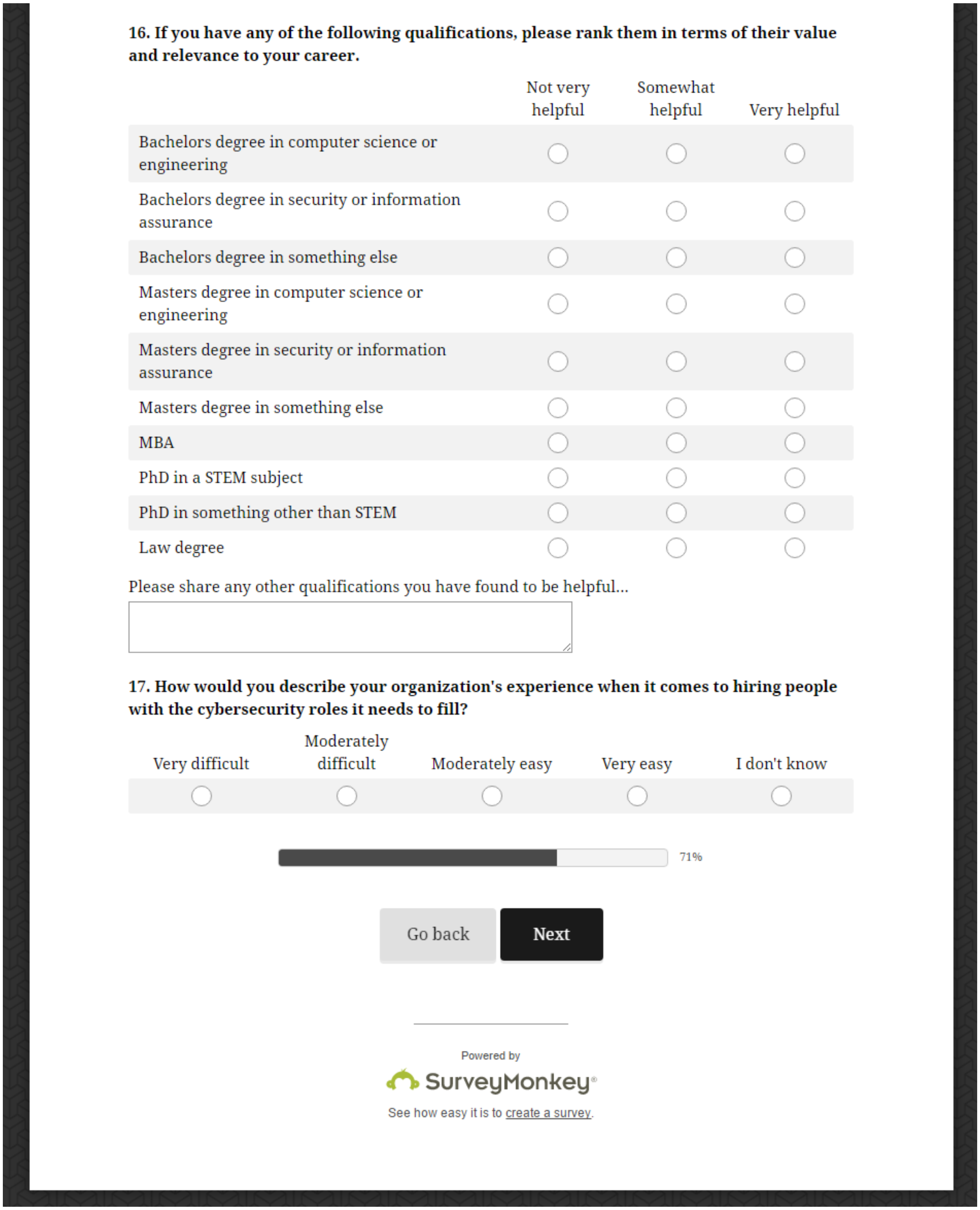
○ Travel

○ Non-profit

15. If you have any of the following certifications, please rank them based on their value and relevance to your career.

	Not very helpful	Somewhat helpful	Very helpful
CISSP	○	○	○
SSCP	○	○	○
Other (ISC)2 certification	○	○	○
Security+	○	○	○
Other CompTIA certification	○	○	○
GSEC	○	○	○
GSE	○	○	○
GISP	○	○	○
Other GIAC certification	○	○	○
CISM	○	○	○
CISA	○	○	○
CRISC	○	○	○
CEH	○	○	○

Please share any other certifications that you found helpful



16. If you have any of the following qualifications, please rank them in terms of their value and relevance to your career.

	Not very helpful	Somewhat helpful	Very helpful
Bachelors degree in computer science or engineering	○	○	○
Bachelors degree in security or information assurance	○	○	○
Bachelors degree in something else	○	○	○
Masters degree in computer science or engineering	○	○	○
Masters degree in security or information assurance	○	○	○
Masters degree in something else	○	○	○
MBA	○	○	○
PhD in a STEM subject	○	○	○
PhD in something other than STEM	○	○	○
Law degree	○	○	○

Please share any other qualifications you have found to be helpful...

17. How would you describe your organization's experience when it comes to hiring people with the cybersecurity roles it needs to fill?

Very difficult	Moderately difficult	Moderately easy	Very easy	I don't know
○	○	○	○	○

And finally, more about you...

Please read: Personality traits vary greatly from person to person, but how much do they vary within a profession? Exploring this subject can help people find work roles they enjoy and at which they excel. The following questions are from a widely used personality survey. There are no wrong or right answers. Try not to "overthink" your responses. Just answer as you see yourself in the moment, not as you might want to be in the future.

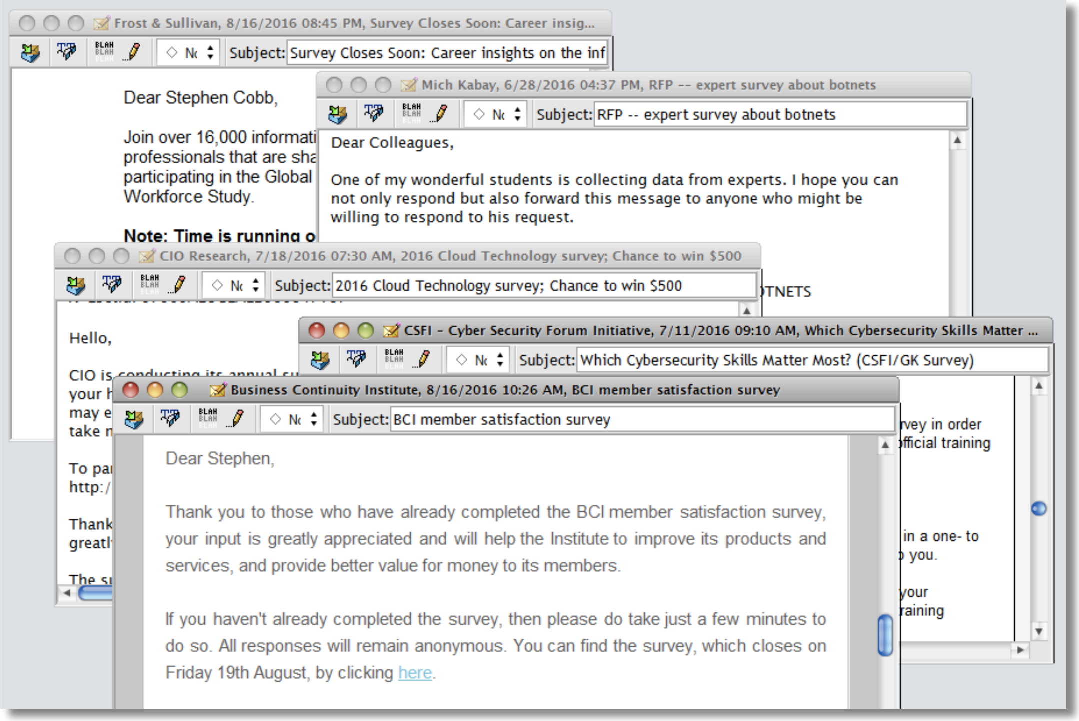
(Survey Monkey does not have the ability to display your traits based on your input here, but you can use a very similar tool to explore your personality traits at this University of Cambridge website)

18. How accurate are each of the following statements as a description of you?

	Very inaccurate		Neither accurate nor inaccurate		Very accurate
I often feel blue.	○	○	○	○	○
I radiate joy.	○	○	○	○	○
I worry about things.	○	○	○	○	○
I trust others.	○	○	○	○	○
I love to help others.	○	○	○	○	○
I believe in the importance of art.	○	○	○	○	○
I love a good fight.	○	○	○	○	○
I experience my emotions intensely.	○	○	○	○	○
I sympathize with the homeless.	○	○	○	○	○
I go on binges.	○	○	○	○	○
I am always prepared.	○	○	○	○	○
I prefer variety to routine.	○	○	○	○	○
I panic easily.	○	○	○	○	○
I take charge.	○	○	○	○	○
I use others for my own ends.	○	○	○	○	○
I love excitement.	○	○	○	○	○
I make friends easily.	○	○	○	○	○
I love to read challenging material.	○	○	○	○	○
I have a vivid imagination.	○	○	○	○	○
I work hard.	○	○	○	○	○
I am always busy.	○	○	○	○	○
I like to tidy up.	○	○	○	○	○
I find it difficult to approach others.	○	○	○	○	○
I keep my promises.	○	○	○	○	○
I get angry easily.	○	○	○	○	○
I complete tasks successfully.	○	○	○	○	○
I believe there is no absolute right and wrong.	○	○	○	○	○
I love large parties.	○	○	○	○	○
I jump into things without thinking.	○	○	○	○	○
I believe that I am better than others.	○	○	○	○	○

Appendix D: Surveys invitations, Summer 2016

Figure 5: Invitations via personal email account (*N* = 5)



Frost & Sullivan, 8/16/2016 08:45 PM, Survey Closes Soon: Career insig...

Subject: Survey Closes Soon: Career insights on the inf

Dear Stephen Cobb,

Join over 16,000 informati
professionals that are sha
participating in the Global
Workforce Study.

Note: Time is running o

Mich Kabay, 6/28/2016 04:37 PM, RFP -- expert survey about botnets

Subject: RFP -- expert survey about botnets

Dear Colleagues,

One of my wonderful students is collecting data from experts. I hope you can not only respond but also forward this message to anyone who might be willing to respond to his request.

TNETS

CIO Research, 7/18/2016 07:30 AM, 2016 Cloud Technology survey; Chance to win $500

Subject: 2016 Cloud Technology survey; Chance to win $500

Hello,

CIO is conducting its annual su
your I
may e
take r

To pai
http:/

Thank
greatl

The s

CSFI - Cyber Security Forum Initiative, 7/11/2016 09:10 AM, Which Cybersecurity Skills Matter ...

Subject: Which Cybersecurity Skills Matter Most? (CSFI/GK Survey)

rvey in order
fficial training

in a one- to
you.

your
raining

Business Continuity Institute, 8/16/2016 10:26 AM, BCI member satisfaction survey

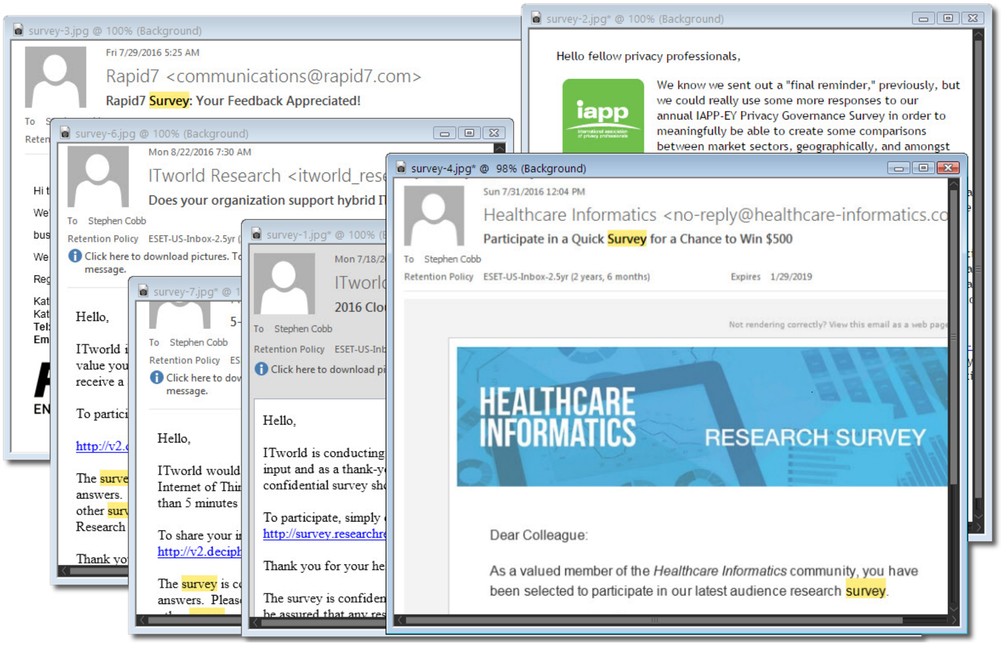
Subject: BCI member satisfaction survey

Dear Stephen,

Thank you to those who have already completed the BCI member satisfaction survey, your input is greatly appreciated and will help the Institute to improve its products and services, and provide better value for money to its members.

If you haven't already completed the survey, then please do take just a few minutes to do so. All responses will remain anonymous. You can find the survey, which closes on Friday 19th August, by clicking here.

Figure 6: Invitations via work email account (*N* = 6)



survey-3.jpg @ 100% (Background)

Fri 7/29/2016 5:25 AM

Rapid7 <communications@rapid7.com>

Rapid7 Survey: Your Feedback Appreciated!

To S

Reten

Hi t
We
bus
We
Reg
Kat
Kat
Tel:
Em

EN

survey-6.jpg @ 100% (Background)

Mon 8/22/2016 7:30 AM

ITworld Research <itworld_rese

Does your organization support hybrid IT

To Stephen Cobb

Retention Policy ESET-US-Inbox-2.5yr (

Click here to download pictures. To
message.

Hello,

ITworld i
value you
receive a

To partici

http://v2.

The surve
answers.
other surv
Research

Thank yo

survey-7.jpg* @ 1

5-

To Stephen Cobb

Retention Policy ES

Click here to dow
message.

Hello,

ITworld would
Internet of Thin
than 5 minutes

To share your in
http://v2.deciph

The survey is co
answers. Pleas

survey-1.jpg* @ 100% (

Mon 7/18/2

ITworld

2016 Clou

To Stephen Cobb

Retention Policy ESET-US-Inb

Click here to download pi

Hello,

ITworld is conducting
input and as a thank-y
confidential survey sho

To participate, simply
http://survey.researchr

Thank you for your he

The survey is confiden
be assured that any res

survey-2.jpg* @ 100% (Background)

Hello fellow privacy professionals,

We know we sent out a "final reminder," previously, but we could really use some more responses to our annual IAPP-EY Privacy Governance Survey in order to meaningfully be able to create some comparisons between market sectors, geographically, and amongst

survey-4.jpg* @ 98% (Background)

Sun 7/31/2016 12:04 PM

Healthcare Informatics <no-reply@healthcare-informatics.co

Participate in a Quick Survey for a Chance to Win $500

To Stephen Cobb

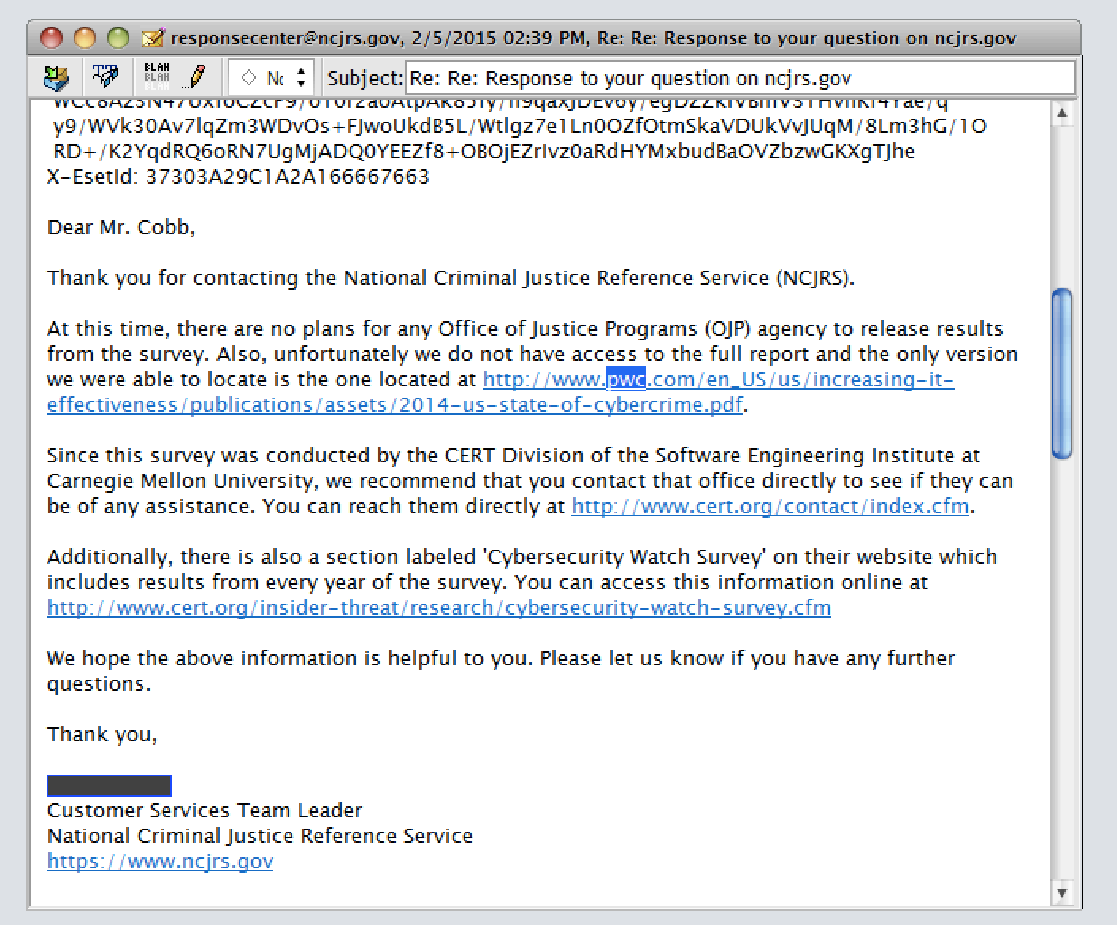
Retention Policy ESET-US-Inbox-2.5yr (2 years, 6 months) Expires 1/29/2019

Not rendering correctly? View this email as a web page

Dear Colleague:

As a valued member of the *Healthcare Informatics* community, you have been selected to participate in our latest audience research survey.

Appendix E: Correspondence with NCJRS


responsecenter@ncjrs.gov, 2/5/2015 02:39 PM, Re: Re: Response to your question on ncjrs.gov
BLAH BLAH BLAH
◇ Nc

Subject: Re: Re: Response to your question on ncjrs.gov

y9/WVk30Av7lqZm3WDvOs+FJwoUkdB5L/Wtlgz7e1Ln0OZfOtmSkaVDUkVvJUqM/8Lm3hG/1O
RD+/K2YqdRQ6oRN7UgMjADQ0YEEZf8+OBOjEZrIvz0aRdHYMxbudBaOVZbzwGKXgTJhe
X-EsetId: 37303A29C1A2A166667663

Dear Mr. Cobb,

Thank you for contacting the National Criminal Justice Reference Service (NCJRS).

At this time, there are no plans for any Office of Justice Programs (OJP) agency to release results from the survey. Also, unfortunately we do not have access to the full report and the only version we were able to locate is the one located at http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf.

Since this survey was conducted by the CERT Division of the Software Engineering Institute at Carnegie Mellon University, we recommend that you contact that office directly to see if they can be of any assistance. You can reach them directly at http://www.cert.org/contact/index.cfm.

Additionally, there is also a section labeled 'Cybersecurity Watch Survey' on their website which includes results from every year of the survey. You can access this information online at http://www.cert.org/insider-threat/research/cybersecurity-watch-survey.cfm

We hope the above information is helpful to you. Please let us know if you have any further questions.

Thank you,

[redacted]
Customer Services Team Leader
National Criminal Justice Reference Service
https://www.ncjrs.gov

Dedication

This dissertation is dedicated to my parents, Dorothy and Cyril,
lifelong learners who taught me so much.

Acknowledgements

The older you get, the more you realize that most individual accomplishments are a group effort and I want to thank all who helped me along the road to this dissertation, including: my San Diego study buddy Fer and the whole of the USRT; all of the staff in the Criminology Department, particularly our cohort's course tutor, Nick Janicki; my correspondents on the discussion board, notably Steve, Marcus, Rick, and Laxman; my ever-encouraging dissertation supervisor, Gavin Butler; and of course, our Course Convenor Tracey Dodman, who convinced me that this whole thing was a good idea in the first place.

Above all, I want to acknowledge the unwavering support and encouragement of my amazing life partner and eternal best friend, Chey.