Dakota State University

Beadle Scholar

Masters Theses & Doctoral Dissertations

Spring 3-2021

Efficacy of Incident Response Certification in the Workforce

Samuel Jarocki

EFFICACY OF INCIDENT RESPONSECERTIFICATION IN THE WORKFORCE

A dissertation submitted to Dakota State University in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

in

Cyber Operations

March 2021

by

Samuel Jarocki

Dissertation Committee:

Dr. Wayne Pauli
Dr. Richard Hanson
Dr. Alan Stines
Dr. Jack Walters
Dr. Cody Welu

DAKOTA STATE UNIVERSITY®

DISSERTATION APPROVAL FORM

This dissertation is approved as a credible and independent investigation by a candidate for the Doctor of Philosophy degree and is acceptable for meeting the dissertation requirements for this degree. Acceptance of this dissertation does not imply that the conclusions reached by the candidate are necessarily the conclusions of the major department or university.

Student Name: Samuel Jarocki
Dissertation Title: Efficacy of Cyber Security Incident Response Certification in the Workforce

Dissertation Chair/Co-Chair: Dr. Wayne Pauli Date: 4/21/21
Wayne E Pauli

Committee member: Dr. Cody Welu Date: 4/21/21

Committee member: Dr. Jack Walters Date: 4/21/21
Jack H. Walters

Committee member: Dr. Richard Hanson Date: 4/21/2021
Richard Hanson

Committee member: Dr. Alan Stines Date: 4/21/2021
Alan Stines

Original to Office of Graduate Studies and Research
Acid-free copies with written reports to library

Abstract

Numerous cybersecurity certifications are available both commercially and via institutes of higher learning. Hiring managers, recruiters, and personnel accountable for new hires need to make informed decisions when selecting personnel to fill positions. An incident responder or security analyst's role requires near real-time decision-making, pervasive knowledge of the environments they are protecting, and functional situational awareness. This concurrent mixed methods paper studies whether current commercial certifications offered in the cybersecurity realm, particularly incident response, provide useful indicators for a viable hiring candidate.

Managers and non-managers alike do prefer hiring candidates with an incident response certification. Both groups affirmatively believe commercial cybersecurity certified job candidates with that same certification can update, modify, and improve the incident response process. The reasoning for this belief is focused more on tie-breaking and common parlance within the information security analyst domain and less on the ability to perform the job. A practical component within the certification process is valuable, and networking expertise is the primary interest of those seeking qualified incident responders. The qualitative component highlighted soft-skills, such as communication, enthusiasm, critical thinking, and awareness, as sought-after abilities lacking in certification offerings covered within this study.

Keywords; cyber, certification, analysts, incident response, defense, hiring

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction

Background

The canvas for what constitutes an incident responder differs wildly and is reliant on a variety of factors. Depending on an organization's scale, Incident Response (IR) may involve processes, procedures, and technologies from multiple divisions or business units. One organization may leverage a system administrator in performing all duties typically related to the incident responder, such as that of a small business or proprietorship. In contrast, a medium to a large organization may have a dedicated incident response team composed of multiple cells containing an information security analyst, reverse engineers, and infrastructure support.

An incident responder should be able to "perform real-time cyber defense incident handling (e.g., forensic collections, intrusion correlation and tracking, threat analysis, and direct system remediation) tasks" (Newhouse, Keith, Scribner, & Witte, 2017, p. 39). A well-trained incident responder can curtail threats related to identifying theft, information leakage, and cyber espionage by correctly recognizing and thwarting attacks of the human element ("European Union Agency for Network and Information Security [ENISA]," 2018). Security operation centers often have analysts work in tier-levels. Tier-three may have the highest level, more experienced analysts, and tier-one analysts may focus on event processing, annotation, and some rudimentary investigation. Tier-three skillsets are not the expectation of junior or intermediate security specialists.

This study reviews literature related to multiple facets needed to support the accompanying research. The survey component is the primary focus of this study. Analysis of the survey data leverages the knowledge gap in hiring perspective and institutional certifications in cybersecurity defense, action, and reporting. We examined commercial certifications within the information technology spectrum, particularly those that relate to incident response. This selective criterion was due to many field certification choices in IT, the maturity of certifications, value, and effectiveness. The proficiency consideration of the responder based on survey data in this study is entry to intermediate level.

Other significant components detailed within the literature review is the hiring aspect and certification applicability in the field. This study includes a review of hiring frameworks, target audience, and conflicting results from broader spectrum domain studies, such as IT and computer science. This portion of the evaluation was necessary to support the methodology, data collection, and conclusions provided to research commercial cybersecurity certification efficacy within the realm of incident response while considering the whole of cybersecurity and correlation with hiring skilled defenders.

Statement of the Problem

Not having a rigorous study of IR certification effectiveness toward quality candidate selection makes hiring in the IR field challenging; there lies the problem. While there are studies focusing on general IT and network certification efficacy and hiring considerations, there is a lack of academic research regarding the cyber defender in these environments. The speed at which technology changes, the rapidity at which cyber network exploitation leverages vulnerabilities, and the follow-on defensive operations needed to thwart attacks exasperate the stated problem.

There are hundreds of information security certifications (Grover, Reinicke, & Cummings, 2016), and many are useful for IR while not being mainly focused within the IR domain. In 2010 the National Initiative for Cybersecurity Education (NICE) created a framework to describe and evaluate government personnel working in cybersecurity. With contributions from academia, commercial entities, focus groups, and experts in their respective fields, NIST published an updated version of the NICE Framework titled "NIST Special Publication 800-181" (Newhouse et al., 2017). The updated version further articulated the expectations of knowledge, skills, and abilities (KSAs) concerning trained IR personnel in Table 1.

Table 1 NICE Specialty Area for Incident Response

NICE Specialty Area	NICE Specialty Area Definition				
Incident Response (CIR)	Responds to crises or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.				
Work Role ID	Work Role Definition	Work Role	KSAs	Tasks	Capability Indicators
PR-CIR-001	Investigates, analyzes, and responds to cyber incidents within the network environment or enclave.	Cyber Defense Incident Responder	See Appendix A for more information on Knowledge, Skills, Abilities, Tasks, and Table 4 Capability Indicators (Credentials And Certifications) relating to the Specialty Area of Incident Response		

Reprinted from *NIST Special Publication 800-181 National Initiative for Cybersecurity Education (NICE), 2018)*, by B. Newhouse et al., Cybersecurity Workforce Framework

The NICE Framework does provide a detailed level of KSAs required to be a productive member of an IR team, and there are corollary specialty areas that share technical skillsets. An example of a shared skillset would be Cyber Crime Investigator (IN-INV-001), which has a Specialty Area within the NICE Framework (Newhouse et al., 2017) containing separate responsibilities, certifications, and career paths (Yasinsac, Erbacher, Marks, Pollitt, & Sommer, 2003). For example, take just one knowledge requirement stipulated for a cyber investigator, such as "K0110: Knowledge of adversarial tactics, techniques, and procedures". Although the K0110 knowledge item is not present for the IR work role, as defined by this Framework, the awareness of attackers' methods, strategies, and processes would be a boon for any incident responder, as represented in the intermediate capability indicators for the Cyber Defense Incident Responder (National Initiative For Cybersecurity Careers And Studies, 2020). This knowledge may be more tailored to a higher-level defender, not necessarily a requirement for the lower tier, entry-level personnel. Additional familiarity with the strategies, best practices, typical procedures, and collaboration techniques (including document creation) would also be essential to defend complex information technology infrastructures during events (Killcrece, Kossakowski, Ruefle, & Zajicek, 2003).

NIST provides guidance on incident response program establishment and implementation via a detailed set of recommendations in their Special Publication 800-61 "Computer Security Incident Handling Guide" (Cichonski, Millar, Grance, & Scarfone, 2012). Additional requirements by the Department of Defense (DoD) 8570.01M Information Assurance (IA) Workforce Improvement Program defines a Computer Network Defense Incident Responder (CND-IR) as one who "…investigate[s] and analyze[s] all response activities related to cyber incidents" (DoD, 2015). Although the NICE Framework does not explicitly assert which certifications meet the criteria for an IR role, the Department of Defense takes a more declarative path of specificity with acceptable certifications required to gain recognition into a particular job role. Information Assurance Technical (IAT) Level I, being the initial level declared in the 8570.01M manual, list A+, Network+, CCNA Security, or System Security Certified Practitioner (SSCP) as requirements to meet qualifications for a CND-IR (Poe, 2018).

The idea that cyber-related professional certifications create a "false sense of security" (Evans & Reeder, 2010, p. 7) contradicts the combined efforts to articulate requirements for a cyber skill identified in the NICE Framework. This contradiction further evidences the need for additional scholarly examination in this domain. Some researchers also embrace this articulation as a viable means of maintaining a curriculum within post-secondary education institutions

(Knapp, Maurer, & Plachkinova, 2017). Current research exists to evaluate IT-related certifications in a general capacity, and not specifically IR. This research may help determine the practicality of certificates obtained by a candidate (Cegielski, 2004) and includes a framework developed to expressly help in hiring decisions of this nature (D. Scott Hunsinger, Smith, & Winter, 2010).

An initial list of viable certifications pertinent to incident response, either by explicitly addressing it in their literature ("SANS Institute," 2018) or containing elements touted by other commercial vendors (*Cyber Security Education*, 2018) as recommendations for breaking into the Incident Responder job field:

- CCE: Certified Computer Examiner
- CEH: Certified Ethical Hacker
- GCFE: GIAC Certified Forensic Examiner
- GCFA: GIAC Certified Forensic Analyst
- GCIH: GIAC Certified Incident Handler
- GCIA: GIAC Certified Intrusion Analyst
- CCFE: Certified Computer Forensics Examiner
- CPT: Certified Penetration Tester
- CREA: Certified Reverse Engineering Analyst

In addition to the above, the following certifications also meet criterion within the IR realm:

- GREM: GIAC Reverse Engineering Malware ("GIAC Certifications: Cyber Defense," 2020)

- CCNA Cyber Ops (renamed to Cisco Certified CyberOps Associate ("CCNA Cyber Ops," 2020) formally SCYBER ("Cisco," 2016)) or CCNA-Security, A+ and Network+ (Poe, 2018)

- SSCP: System Security Certified Practitioner (DoD, 2015; Poe, 2018)

Table 2 represents the sizeable and prevalent commercial certification vendor (ISC)^2, or the International Information System Security Certification Consortium's prediction of future certification pursuits ((ISC)^2, 2018).

Table 2 Certification Pursuits

CISSP: Certified Information Systems Security Professional	17%
CCSP: Certified Cloud Security Professional	15%
CISSP with Concentration: ISSAP, ISSEP or ISSMP	13%
CSSLP: Certified Secure Software Lifecycle Professional	11%
SSCP: Systems Security Certified Practitioner	11%
CCNA Security: Cisco Certified Network Associate Security	10%
CCNA Cyber Ops: Cisco Certified Network Associate Cyber Ops	10%
CCNP Security: Cisco Certified Network Professional Security	9%
Certified Ethical Hacker	7%
SCYBER: Cisco Cybersecurity Specialist Program	7%
CISM: Certified Information Security Manager	6%
CIW: Certified Internet Webmaster Security Analyst	6%
CompTIA Security+	5%

Reprinted from *Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens. (2018),* by Cybersecurity Workforce Study, (ISC)^2.

Note for transparency and interests, (ISC)^2 is the security organization that administers the top five entries in Table 2. (ISC) ^{2} and the business organization that offers the SSCP certification path that meets DoD 8570.01M requirements.

This paper's mixed-methods approach studies the practical relevance of IR specialized duties and the need for qualified personnel in the IR domain. We review current perceptions of certification effectiveness in the workforce and certifications when making hiring decisions. Lastly, this paper examines capabilities and overall utilization of resources to meet operational objectives, as practiced in multidisciplinary incident response fields outside of cybersecurity, such as emergency response management (Chen & Sharma, 2012, p. 2), medical systems, nuclear power plant operations, and military response teams (Steinke et al., 2015, p. 21).

Purpose of the Research Study

The purpose of this study was to examine whether the effectiveness of an assortment of industry certification offerings available to individuals starting in the incident response domain has any bearing on hiring choices. There exists a myriad of courses, paths, and formats in obtaining certifications. Techniques and structures currently available consist of traditional classroom-based instruction, eLearning, interactive online mechanisms with pre-recorded and live offerings supporting audio and video playback, and various combinations (CompTIA, 2020).

This paper will study what constitutes adequate knowledge garnered from certification completion that can help select certificate holding individuals for hiring purposes and the format of the learning approach[es] available. The examination includes supporting dependent data surrounding certification contributions in performing an incident responder's role based on certifications held by a candidate and those qualified to assess their effectiveness.

Research Questions and Hypotheses

The hypothesis for this study will be, "Can commercially available incident response cybersecurity certifications be a useful criterion for selection of preliminary incident response (IR) candidates by a hiring entity?" Apart from sampling errors, a null hypothesis proves there does not exist a difference between a population (Oxford English Dictionary). This study's null hypothesis is finding significant evidence that a hiring entity does not prefer hiring candidates with an IR certification.

Primary Quantitative (PQN-n) and Primary Qualitative (PQL-n) questions represent key issues focusing on the stated hypothesis. The following are quantitative and qualitative inquiries based on Hunsinger et al.. hiring framework and initial survey instrument (D. Scott Hunsinger et al., 2010, pp. 13-14, Appendix B). The complete survey presented to respondents is in Appendix C. The following are the research questions for this analysis:

- **PQN-1**: Is a candidate with an incident response specific certification preferred when hiring/recruiting?
- **PQN-2**: Can organizations benefit from IR certified candidates to update, modify, and improve the IR process?
- **PQL-1**: What skills, knowledge, and abilities (KSA's) do you believe an effective incident responder should possess?

Secondary Questions (SQN-n and SQL-n) in Table 3 are ancillary queries to support the primary objective and provide alternate data points for this study and possible future works.

TABLE 3 SECONDARY QUERIES

SQN-1	Job Role of survey respondents
SQN-2	Familiarity with specific IR certifications
SQN-3	Frequency of checking candidates' certification
SQN-4	Ways IR Certification Can Assist in the Hiring Process
SQN-5	Potential Usefulness of Certifications not in IR Domain
SQN-6	Potential Influence on the Value of Certification
SQN-7	Importance of a Practical Component

SQN-8	Importance of Vendor-Specific and Vendor Non -Specific Certifications
SQN-9	Varying Difficulty of IR Response Certifications
SQN-10	Level of Difficulty for Certifications
SQN-11	Potential Benefit of IR Certification for Long Term IR Persons
SQN-12	Potential Benefit to Organization
SQN-13	Likelihood of Recommending IR Certification to Candidate/ Employee
SQL-1	If IR certifications help, elaborate on non-IR skills that may assist a responder
SQL-2	If IR certifications help, elaborate on improving IR processes
SQL-3	If IR certifications help, elaborate on analytical mindset
SQL-4	Training equality for individuals with and without certifications

Independent and Dependent Variables

This study referred to subject matter experts, hiring managers, and recruiters aware of incident response hires' performance aspects as IR Decision Makers (IRDM). The independent variable is the certification held by the candidate or [potential] employee. The dependent variable is the incident responder's hiring choice. Measurement of the variables occurs via qualitative and quantitative evaluation based on their efficacy assessment.

Theoretical and Conceptual Frameworks for the Research Study

The components for achieving abstract concepts relevant to this study relied on the following contributing theories, guides, and frameworks detailed in the literature review:

- Cybersecurity Framework v1.1 (NIST, 2014)
- NIST Special Publication 800-181 revision 1, the Workforce Framework for Cybersecurity (NICE Framework) (Newhouse et al., 2017)
- A Framework of the Use of Certifications by Hiring Personnel in IT Hiring Decisions (D. Scott Hunsinger et al., 2010), modified for incident response.

The process employed for data collection was inferring quantitative data through statistical analysis, parallel with coding the themes for limited qualitative results (Subedi, 2016). The majority of collected data for the survey is quantitative. The two-part collection assessment methodology (further detailed in Chapter 3: Research Methodology | Data Collection) was via data triangulation (Denzin, 1978).

Definition of Terms

There exists a differentiation of names, and in some instances, function between various incident response organizations. A 'security operations center' (SOC) may focus on a more technical level, with a higher degree of networking prominence, while dealing with the mitigation and remediation aspects. A 'computer emergency response team' (CERT) may interact with internal and external entities to share indicators of compromise (IoC) and intelligence distribution responsibilities. This collaboration works toward identifying and preventing security incidents from occurring. A 'computer security incident response team' (CSIRT) answers events from a technical standpoint and leverages business processes that incorporate risk awareness and communication (Ramilli, 2018). These three iterations of IR entities are just a few titles used in industry and government – additional combinations exist utilizing synonymic words and phrases to include capability and handling (Andrade & Yoo, 2019; Ruefle, 2007). These terms will differ based on the breadth and depth exhibited by a team or multiple groups. For this study, operational response teams' names are considered identical within the overall function of where an incident responder would work.

Like variations with SOC naming and function, there are multiple names for the incident responder role that may incorporate network defense, information security analyst, and defender. This study may use any permutation of the preceding terms to represent the incident responder.

Cybersecurity and information security are also terms used interchangeably throughout this study. The relationship between the vulnerable threats to information and communication technology in the cybersecurity realm and the storage and transmission of assets as part of information security (Von Solms & Van Niekerk, 2013) are both the focus of IR, and ultimately the Incident Response Decision Maker (IRDM) when choosing candidates.

Assumptions and Scale

Basic cybersecurity practices are required regardless of an organization's size, and consequently, the varying skills needed by an incident responder specific to the organization's business line. There will be a significant disparity among the number of hosts on an enterprise network, including security appliances and monitoring hardware between organizations. Purpose-built data centers and organizations may focus on industrial control systems, business, and finance. Each variance of function would require specific expertise to defend against cyberattacks. The same discrepancy may hold for the number of users, the roles and responsibilities, and contribution to each user's overall cybersecurity effort. An enterprise may have user volumes from single digits to millions. Users may have the least privilege practices in place (Schneider, 2003), limiting their ability to make IT assets changes or have full administrator rights across the organization. Size, scope, breadth, and depth of user differences are outside the scope of this study.

IR certifications that meet entry and intermediate level criteria change continuously. Cybersecurity is an ever-evolving field, so too is the sub-component of defense that logically track with the abilities and sophistication from the offensive components of vulnerability analysis, computer system, and network exploitation (Andres, 2012, p. 91). Industry and government criteria, regulations, and manuals must keep pace with constant changes in IT.

Selection and choice will inevitably change; the certification choices presented here are applicable at the time of this study's writing. Table 4 identifies the capability indicators across the Cyber Defense Incident Responder work role (PR-CIR-001) as defined by NICE's Cybersecurity Workforce Framework (National Initiative For Cybersecurity Careers And Studies, 2020). For the full table, see Appendix A, Capability Indicators.

TABLE 4 CAPABILITY INDICATORS (CREDENTIALS AND CERTIFICATIONS)

	Recommended: Yes, **Example Types**: N/A **Example Topics**:
Entry	Certifications addressing new attack vectors (emphasis on cloud computing technology, mobile platforms and tablet computers), new vulnerabilities, existing threats to operating environments, advanced IDS concepts, applications protocols, concepts of TCP/IP and the link layer, DNS, fragmentation, IDS fundamentals and initial deployment (e.g., snort, bro), IDS rules (e.g., snort, bro), IPv6, network architecture and event correlation, network traffic analysis and forensics, packet engineering, silk and other traffic analysis tools, TCP, tcpdump filters, UDP and ICMP, Wireshark fundamentals.
Intermediate	Certifications addressing incident handling (identification, overview and preparation) buffer overflow, client attacks, covering tacks (networks, systems), denial of service attaches, network attacks, password attacks, reconnaissance, scanning (discovery and mapping, techniques, and defense), session hijacking and cache poisoning, techniques for maintaining access, web applications attacks, worms, bots, and bot-nets.
Advanced	Certifications addressing identification of malicious system and user activity, incident response in an enterprise environment, incident response process and framework, timeline artifact analysis, timeline collection, timeline processing, volatile data collection, filesystem structure and analysis, artifact analysis.

Reprinted from *Incident Response. (2020),* by National Initiative for Cybersecurity Careers and Studies.

Scope and Delimitations

We chose incident response as the specific facet of cybersecurity due to its importance in the current IT climate. The numerous and increasing privacy disclosures and hacking victims in past years continue to highlight the need for effective cyber defense and analysis resources in combating and reducing cyberattacks (Federal Trade Commission, 2019; Privacy Rights Clearinghouse, 2019); competent personal play a significant role in this methodology (*U.S. Bureau of Labor Statistics, Employment Projections program*, 2019).

The incident response domain is quite extensive between small, medium, and large businesses. Any declared incident may involve many significant components of an organization where a breach is concerned, such as networking, policy, and operational business units. Business continuity is paramount for success; thus, an adequate response to an incident in maintaining organizational processes is vital, but each entity's specific detail differs considerably (Selznick & LaMacchia, 2017, pp. 218, 225). The boundary and scope of influence could be large or small for IR analysts and is not a determining factor in this study; therefore, we will not assess an organization's size.

Limitations

While the information technology field is vast, the more specific incident response realm, as a subset of cybersecurity, is reasonably smaller to garner quality data. Identifying potential survey respondents within a microcosm of the population with qualifying criteria specified (through logic selection) within the survey instrument is a significant limitation for small studies. Soliciting consensual avenues for a broad survey distribution (e.g., email, social media, SMS), access, and eventual submission require financial resources and potential survey recipients' advanced pooling. Restrictions on survey distribution due to reduced social interaction during a global pandemic may exasperate sample size collection efforts. The researcher recognizes a Type I or Type II error may occur after the completion of data collection. Small sample sizes may result in a finding to be statistically significant due to chance (false positive) or not found to be statistically significant (false negative) (Hamill, 2019). Hamill points out an additional factor in “Multiple Hypothesis Testing and False Discovery Rate - Type I and Type II errors” because Type II errors may occur if the subjects have a high degree of inconsistency. Qualifier questions help reduce this error type, specifically adding queries on job roles, positive interaction, and direct observation of a candidate's incident response activities.

The survey instrument addresses internal validity by considering qualifications and endorsements a person may have with random selection representing the population studied (Cuncic, 2020, p. 2). Participants are randomly selected, by their own accord, based on reception of survey and volunteer participation, without disclosure of method or identifying information. There existed no variation in survey protocol; all respondents received the same platform, representation, logic, and content. Respondents were not aware of the a priori hypothesis.

The study's aim was communicated in the first section of the survey qualifier as one factor to recognize and improve external validity (Cuncic, 2020). Group characteristics were not a factor in obtaining data results outside of the majority (>=18 years old). The researcher conducted a field survey at inception to ensure syntactical and logical sentence structure did not hinder comprehension of one or more questions.

The primary researcher is employed in a managerial incident response capacity and practiced rational processes to limit outcome bias by not providing any opinion about perception, results, personal choice, or reflection of any survey question or topic. The research did not discuss the rationale, personal preference and carefully ensured survey instrument phrasing did not telegraph a bias against the [null] hypothesis.

Significance

The study benefits information technology and security domain stakeholders toward expectations, value, and return on commercial certifications investment. This study advances the knowledge for use in decision-making in training considerations, potential onboarding candidates, and managing people's expectations and processes relating to cybersecurity accreditations. These practices should include academic research studies to help achieve unbiased selection in certification offerings, personnel, and circumstance. Reliance on commercial entities and vendor literature alone impedes a holistic research view that may compromise selection criteria for conflict of interest.

Chapter Summary

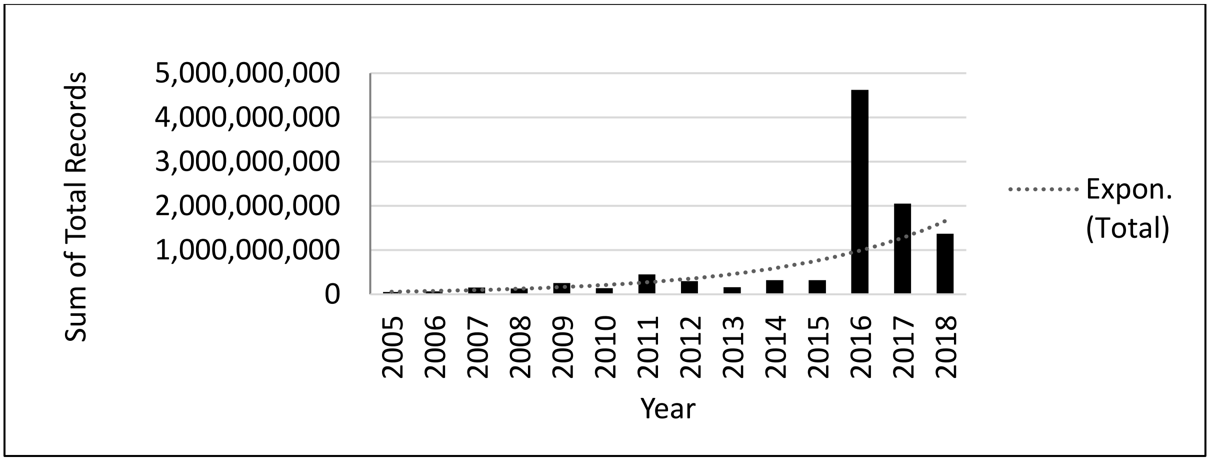
This introduction chapter reviews the research towards practical incident response certifications and hiring practices. IR work is defined for this study to include limitations and significance within the IT domain. We discussed the problem statement and the purpose of the research, including high-level research questions intent and the methodologies employed during data collection and dissemination. Assumptions while conducting this research were articulated as well as the significance of the resulting hypothesis. The following chapter reviews the literature to identify known and unknowns within this topic to build a foundation for the subsequent methodology, data collection, and results.

Chapter 2: Literature Review

Outlook

Data breaches, cyber-crime, and identity-fraud are leading incident-centric examples that have markedly risen since 2015. As early as 2011, data breaches have grown more than sixty percent from one year to the next (Ginovsky, 2012). Privacy Right Clearinghouse sources data from the Department of Health and Human Services and states with laws that allow the Attorney General's office to report raw numbers. Figure 1 depicts data breach trending by the number of records from 2005 to 2018 (Privacy Rights Clearinghouse, 2019). Over time, these record summations include all types of data breaches, ranging from hacking, and insider threats, to portable device attacks and unintended disclosures.

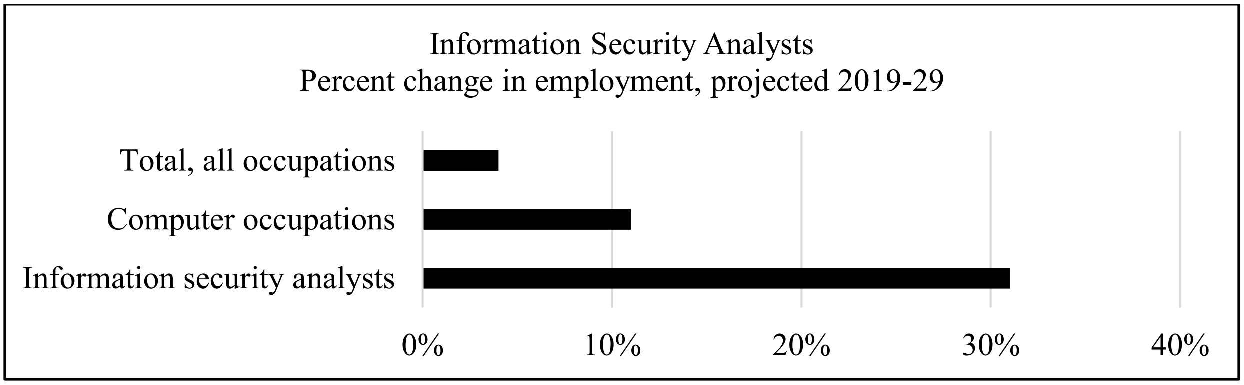
FIGURE 1 CHRONOLOGY OF DATA BREACHES



Cyber-crimes' lucrative returns, highly congested legal systems for prosecution, convenience, and diminished chances of getting caught (Kshetri, 2009) solidify criminals' incentive to persist in this type of crime. The number of identity-fraud related reports to the Federal Trade Commission from 2001-2019 has increased nearly ten-fold, from 0.33 million to 3.20 million (Federal Trade Commission, 2019). Based on a recent, comprehensive study of data breaches from 1990 to the first quarter of 2019, malicious capture of personally identifiable information (PII) represents most data breaches at 65% (Hogan, Olson, & Angelina, 2020, p. 25). These statistics on the position of cybersecurity-related incidents for the foreseeable future indicate an upward trend that will require responses by qualified and competent personnel to keep organizations' data and information systems safe from adversaries.

Within the federal government, many agencies failed to "effectively [respond] to cyber incidents"; and cited inadequately qualified personnel and training as reasons for failures (Wilshusen, 2014, p. 2). Within the larger, more encompassing field of information security and analytics, an estimated 1.5 million skilled cybersecurity jobs may be needed by 2020 (Sarkar, 2015). An information security analyst's outlook, which encompasses incident responders, is projected to grow thirty-one percent between 2019-2029, as depicted in Figure 2, which is significantly larger than that of all other occupations at four percent (*U.S. Bureau of Labor Statistics, Employment Projections program*, 2019).

FIGURE 2 EMPLOYMENT OF INFORMATION SECURITY ANALYSTS



Reprinted from *Occupational Outlook Handbook, Information Security Analysts. (2019),* by Bureau of Labor Statistics, US Department of Labor.

Another facet of this response arena when evaluating the need for first responders is information assurance (IA), particularly in the role of protecting critical infrastructure defined in the National Incident Response Plan (NIST, 2014), which represents a culmination of response and policies regarding the protection of an organizations infrastructure. Multiple frameworks exist in the IA discipline, closely related to the procedural elements for incident response and attack prevention. Increasing security breaches year after year, various aspects of information security requirements, and potential growth and trends in the IR service market ("Research and Markets," 2018; *U.S. Bureau of Labor Statistics, Employment Projections program*, 2019) have consequences. These surges put an ever-increasing burden on hiring qualified and capable personnel to provide commensurate response services to fulfill these needs.

Certification

Limitations

Analysis of overarching IT certifications is central to related studies in the cybersecurity field. The myriad of sub-domains within cyber and information security, notably information security analysis to include incident response, is considerably limited in scope (Selznick & LaMacchia, 2017, p. 249; Von Solms & Van Niekerk, 2013, p. 101). Timeframes of typical certification courses range from days to weeks of in-person instruction -- if that option is available or offered. Alternate, or sometimes included with live instruction, is a juxtaposition of many learning options. A fusion of technology is frequently employed, ranging from online reading, interactive labs, exercises, challenges, forums, test banks, and one-on-one or group communications (CompTIA, 2020).

The benefits of formal education compared to commercial certifications, and whether the latter is perceived as required for employment (Lasheen, 2015), is outside this essay. Considering the problem statement of whether field-specific certifications are an effective instrument to gauge good candidacy, the employer or credentials evaluator will address requisite certification holding(s) of commercial certifications. This study's perception and value of an IR endorsement from the candidate's point-of-view are not applicable.

Certification Maturity

Utilization of information technology (IT) certifications, from as early as 1989, are in use to introduce, reinforce, and assess individuals and groups from countries across the world (Adelman, 2000). Vendors, such as Novel, had myopically focused certifications; in contrast were comprehensive examinations in the considerable field of computing, from as back as 1973 (Wierschem, Zhang, & Johnston, 2010, p. 89). Commercial and government entities must adjust their curriculum and certification criteria to keep pace with ever-evolving technologies and threats (Reid, 2012).

Commercial vendor offerings meet requirements defined for each iteration of the NIST framework (NIST, 2014) and the DoD 8570.01M requirements and its predecessor, DoD 8140.01 (DoD, 2015). These constraints provide further unification, keeping pace with changes in policies, audits, technologies, and requirements (Bartlett, Horwitz, Ipe, & Liu, 2005, p. 52; DoD, 2015, p. 44; Poe, 2018, p. 78).

Value and Effectiveness

For those respondents who had a declared role in observing, hiring, or selecting an employee or current colleague who has obtained an IR-related certification, the ultimate question is whether the IRDM considers the certification valuable. Ancillary results based on whether a hands-on or practical approach is considered more effective was not available for dissemination. Questions are toward those with certifications to comment on the perceived level of difficulty, benefit, and whether the IRDM preferred a certificate holding candidate.

Pierce’s phenomenological IT study found value in vendor-specific certifications and preference with vendor-neutral certifications (Pierce, 2009). Highly definitive, vendor-centric training from the certificate earner would logically isolate the achievement within a myopic system or process, reducing the perceived value to potential employers that do not utilize the explicit vendor(s). Pierce's study also found mixed responses, such that the certification process was an incumbrance, while still being a reliable foundation for relevance in the field (Pierce, 2009).

Bartlett's study concerning commercial credentials' perception in the IT field eighteen years ago indicated a strong correlation between IT certification holders and ease of recruitment in time efficiency and cost reduction (Bartlett, 2002, p. 26).

Table 5 shows a recent survey by Benslimane et al. finding an average of 78% "required or desired" knowledge by analysts and managers in the following certifications (Benslimane, Yang, & Bahli, 2016, p. 4):

TABLE 5 IMPORTANCE OF PROFESSIONAL CERTIFICATIONS

	Analyst	Manager	Total
CISSP	25	40	65
CISM	11	26	37
GIAC Security Essentials	12	14	26
CISA	10	14	24
CEH	5	5	10
Security +	5	3	8
GIAC GCIH	6	1	7
Other GIAC certifications	12	6	18
Various Cisco certifications	7	8	15
Various Microsoft certifications	7	6	13

Reprinted from *Information Security between Standards, Certifications and Technologies: An Empirical Study. (2016),* by Benslimane, Y., Yang, Z., & Bahli, B, 2016 International Conference on Information Science and Security (ICISS): IEEE.

To be a beneficial certification in the defender, responder, and analyst role; and determine the best course of action against an intruder or adversary, practical components for successful certification awarding are necessary (Reid, 2012). A 2017 UK study rates the following assessment methods overall effectiveness, from high to low: virtual labs, oral exams, employment history to include qualification review, narrated paper-based exams, and finally, multiple-choice paper-based exams (Knowles, Such, Gouglidis, Misra, & Rashid, 2017). The inclusion of practical, kinetic options such as working in a lab environment or speaking on a subject to demonstrate mastery ranks higher than written skills assessment.

During premier cyber exercises, notably Cyber Shield, reduced *time-to-detect* (TTD) was seen for those possessing Security+, but not for those with A+ and Network+ certifications; instead, their *time-to-end* (TTE) was reduced (Henshel, Deckard, & Buchler, 2016). TTE is the time at which an analyst detects an event and acts to resolve the potential incident. The reduction may originate from a deficiency in "clean monitoring data" or overly cautious respondents, and Henshel et al. 's data oppose at times what would seem logical; Security+ certification holders should have better performance, but that was not always the case. Additionally, the participants believed that comprehending their job was more advantageous than information security certifications (Henshel et al., 2016, p. 6). These contradictory results are an example of the difficulty in assessing current studies in the IR field.

Hiring Aspect

Hiring managers and influencers to the hiring process must consider numerous factors that differ based on field applicability. Some considerations are generalized, such as degree level and on-the-job experience; others are more detailed for the sector in which an organization seeks qualified personnel. With the tremendous outlook for IT and security-related jobs (*U.S. Bureau* *of Labor Statistics, Employment Projections program*, 2019), a methodology for filtering potential hires can narrow choices and reduce technological competencies for recruiters spanning multiple job fields. Assessing certification efficacy may provide an additional element of consideration during the hiring phase.

The target audience consists of individuals involved with the hiring and observing employees and candidates who participate in a certification endeavor. Current research detailing cybersecurity, which an incident responder (analyst) incorporates, is seen from studies in hiring frameworks particular to decisions on whether candidates holding skill-related accreditation is accounted for while offering employment (D. Scott Hunsinger et al., 2010). Vendor-specific vs. vendor-neutral certification may play a role in the initial hiring of a prospective responder and whether that individual has the potential for promotability (Gleghorn & Gordon, 2012, p. 16). Because the talent pool is deficient, selecting candidates possessing one or more certifications may be a deciding factor (Poe, 2018).

There exist conflicting results from survey respondents for research studies focusing on the IT Security realm. Hunsinger notes C-level associates would hire inexperienced people with certifications, while others required certifications for consideration. Even amongst managers, some believed certifications were nothing but the ability to "pass a test" (David Scott Hunsinger, 2005, p. 14).

Human capital, such as the essence of an individual's knowledge, experience, and skills (Goldin, 2014), uses an overall trait characteristic as one aspect in pairing an individual to a specific role. Early findings from 2002 show that human resources perceived traditional four-year degree holders as ideal but recognized IT-centric certifications as assistive in decision making for candidate selection and cost-saving for the employer (Bartlett, 2002). Another early finding from industry professionals in information technology was certification not correlating with aptitude, nor should it be utilized for hiring (Cegielski, 2004), although the practice continues (Bartlett et al., 2005).

Resources

The basis of this research study originated from the following publication:

Jarocki, S., & Kettani, H. (2019, 4-6 May 2019). *Examining the Efficacy of Commercial Cyber Security Certifications for Information Security Analysts*. Paper presented at the 2019 4th International Conference on Information Systems Engineering (ICISE).

Chapter Summary

This literature review chapter explores sources detailing the many facets of incident response certification within the scope of hiring decisions. Ever-increasing data breaches in the multitude of forms those breaches take – from quintessential hacking to insider threats, highlight the need for competent defenders. Lucrative returns on investment from cybercriminal activity are contrary to a reduced outlook for future cyber-crimes and data breaches.

The history of IT certifications goes back more than four decades, with NIST and the DoD having contributed to identifying which certifications cover the IT domain's subfields. Resources for the cornerstone of this study's significance in IR certifications value and effectiveness regarding hiring are lacking, but there were corollary studies for generic IT fields.

From certification value to hiring choices, we reviewed multiple tangents with varying results. Pierce's study found the IT certification process inconvenient but relevant. Bartlett’s study touted the improved recruitment aspect by certification owners. Henshel et al. saw results-based inconsistencies between popular, introductory certifications Security+, A+, and Network+ (all available through CompTIA vendor). Hunsinger notes inexperience and test-taking abilities as negatives even with a certification, but still useful when considering employment.

The following research methodology chapter will discuss the mixed methods design and detail the instrumentation and data collection processes of this study.

Chapter 3: Research Methodology

The purpose of this study is to address whether commercial cybersecurity certifications for incident responders affect hiring choices. This paper will employ an explanatory concurrent mixed methods design, simultaneously collecting quantitative and qualitative data. Data collection occurs via a survey instrument collected from approximately fifty participants familiar with cybersecurity Information Security Analysis, particularly those fulfilling the role of hiring managers, influencers, or candidate recruiters to test the efficacy of certifications in incident response. The purpose of data collection is to assess whether a candidate's knowledge, skills, and abilities are adequate for hiring based on content and testing for certification(s) earned. The qualitative portion provides additional insight into quantitative results to explore the background, familiarity, and circumstances of individuals' incident response fulfillment within a security operation center.

Mixed-Methods Research

The foundations of a mixed methodology framework as a means of inquiry into a research question contain triangulation, multiplism, mixing methods, and paradigms (Greene, Caracelli, & Graham, 1989, pp. 256-257, 264). The basis of implementing triangulation within research design, proposed by Denzin, introduced four distinct triangulation types: data, investigator, theoretical, and methodological (Denzin, 1978, p. 43), all centered on improving its validity.

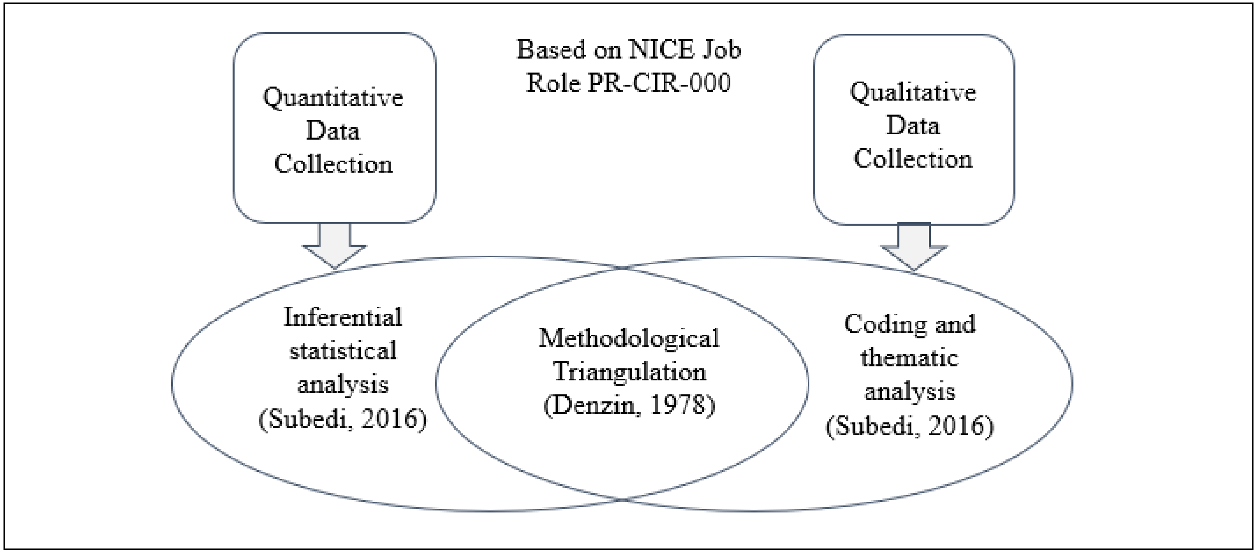
With only two data sources in this research design choice assisting the investigator in data triangulation, multiple principal or secondary investigators will not be a factor for this study. Some grounded theory components within the qualitative phase are not relevant as the data set size is small (less than 100 participants) (Denzin, 1978, p. 239). There are minimal survey questions that require a specific conceptualization of coding data (PQL-1 and SQL-1). Most text entries follow the form of enhancement, clarification, or explanation of the current survey item. These short entries will not be available for each item that allows input since the qualitative query may not facilitate a more in-depth answer. We will not be employing theoretical triangulation due to coherent and committed theories included in this study (Denzin, 1978, p. 251; Mathison, 1988, p. 13).

A cornerstone of this research will center on using multiple methods to reach valid and thoroughly assessed conclusions as defined by methodological triangulation (Denzin, 1978, p. 289). As Mathison points out, the triangulation strategy is just that, a strategy. By incorporating:

- a convergence of data [sources] and methods
- realization of inconsistency and a possible contradiction of data while generating an all-inclusive understanding of the phenomena under scrutiny (Mathison, 1988, p. 15)
- bias reduction of inquiry, context, and substantive theory such as "…identifying differences and similarities of contextualized instances, and patterns, across and within case studies focused on a similar theme ("Encyclopedia of Case Study Research," 2010, p. 907)"

which can further enhance or validate the data and supporting theories (Greene et al., 1989, p. 256). The strategies in Figure 3 will help determine if incident response certifications are valid within the research questions' parameters and help qualify which skills an IR should have to be useful from an IRDM’s perspective.

FIGURE 3 RESEARCH MODEL - EXPLANATORY CONCURRENT MIXED METHODS DESIGN


Based on NICE Job Role PR-CIR-000
Quantitative Data Collection
Qualitative Data Collection
Inferential statistical analysis (Subedi, 2016)
Methodological Triangulation (Denzin, 1978)
Coding and thematic analysis (Subedi, 2016)

Examination for the efficacy of commercial cybersecurity certification, wherein which cyber incident response is the focus, will utilize an explanatory concurrent mixed method design approach. A single quantitatively designed study would not be sufficient to capture, articulate, and thoroughly research, triangulate fully, and validate (Pritchard, 2017, p. 54). The survey instrument's beginning focuses on individuals with subject matter expertise (SME) in the incident response domain. The respondents can provide expert opinions on requisite knowledge required to perform (in a starting capacity) the highly technical and analytically driven functions of an incident responder. Hiring managers and recruiters are similarly a target population in determining whether candidates have demonstrated sufficient practical approaches to fulfilling essential roles. The National Institutes of Standards' (NIST) National Initiative for Cybersecurity Education (NICE) framework articulates each category and role. The knowledge, skills, and abilities (KSAs) within the "Protect and Defend (PR)" category further define the specialty area of the Incident Response (CIR) work role PR-CIR-001 (Newhouse et al., 2017, pp. 20, 111).

The recruitment of analytically minded candidates who can fulfill incident response (IR) duties is challenging based on the lack of qualified responders (Gonzalez, Kossakowski, & Wiik, 2005, p. 3). An additional challenge is the length of time and dedication required to learn and collaborate effectively from past incidents (Ahmad, Hadgkiss, & Ruighaver, 2012, p. 649; Van der Kleij, Kleinhuis, & Young, 2017, p. 7). A candidate may possess theoretical knowledge, but lack the practical and analytical skills to determine proper steps during an incident while performing Cybersecurity Framework functions during an incident, such as Identify, Protect, Detect, Respond, and Recover (NIST, 2014). This researcher aims to determine if commercial cybersecurity certifications specific to the incident response (information security analysis) domain effectively choose capable responders for security operation center (SOC) positions. This study aims to utilize an explanatory concurrent mixed-method design that collects hiring managers, recruiters, and subject matter experts' (SME) input with a quantitative survey instrument containing qualitative questions and respondents' opportunity to elaborate on an answer. This study will focus more strongly on quantitative data with a qualitative follow-up instrument to explain numerical results within the qualitative data (John W Creswell, 2014), notated as QUAN + qual, rather than the first quantitative aspect as a single manageable research method.

The quantitative phase will explore the relationship between IRDM and candidate abilities to fulfill IR tasks. The data collection is observational, and no manipulation occurs to the independent variable through correlational non-experimental design (*Quantitative Approaches - Center for Innovation in Research and Teaching*, 2019). The follow-on questions focus on discovering how the quantitative survey instrument results further delve into the emerging theories utilizing a grounded theory approach. The qualitative data analysis section of the methodology section will elaborate on steps and coding necessary after data collection.

Role of the Researcher

The researcher is employed in an incident response capacity and has an ongoing relationship with individuals in the same field. While the area is vast and geographically distanced, the researcher's questions shall not influence the answers the researcher may come across during this study to avoid tainting the results' validity. In this capacity, the researcher's role is to provide respondents with survey instruments and collect follow-up data through questioning [via the survey instrument] for clarification.

Instrumentation

It is imperative to consider survey design in reducing the chances of measurement error. This practice helps reduce survey misinterpretation, question skipping, and inaccurate answers (Collins, 2003).

Participant Selection and Sample Size

Limitations exist for choosing respondents to those that meet the criteria of an IRDM, as previously defined. Viable study participant consideration is to individuals who have had a substantial role in interviewing, questioning, observing, and identifying candidates' performance indicators. The survey instrument will ask for these metrics as a vetting procedure:

- The applicant’s job role.
- The participant's involvement in observing, hiring, or selecting a candidate who has obtained an Incident Response (IR) related certification.
- The participant's familiarity with a list of certification listings related to the IR domain.

These are initial queries that ensure the remaining questions are pertinent to the research; any negative responses to the above will trigger an end to the survey. These elimination questions are for the efficiency of time for both the researcher and the participant. This vetting also increases the validity and decreases coding errors. As a general guideline, the sample size was in the twenty to thirty range (John W Creswell, 2014), with an optimistic count of one-hundred with time considerations. The largest sample size was for the quantitative portion of the survey instrument at seventy-three, with sixty-two as the count for qualitative responses.

Pilot-testing and Initial Survey Instrument Development

The primary researcher provided the survey instrument to incident response analysts or managers. Through a web-based survey, the survey's interaction assessed analytical capabilities for a real-world type of incident exploration and dissemination by a potential or already onboard SOC analyst. After the initial screening questions, the participants progress toward specific questions regarding their input on candidate selection certification efficacy and usage. The qualitative section of the survey leverages the quantitively-based queries to elicit responses needed in addressing follow-on questions, based on a hiring and personnel framework by Hunsinger et al., detailed in Appendix B, Figure 10 Factors influencing the use of IT certification in hiring in (D. Scott Hunsinger et al., 2010).

Follow-Up Survey Construction

Constant iterations were necessary to develop a viable survey instrument that is as error-free as possible. Pretesting was essential to flush out problems, minimize errors, and identify failed or refused survey responses. Presser et al. state that even with careful pilots and pretesting, "…conventional pretesting would still be [ill-suited] to uncovering many questionnaire problems". An introduction of cognitive interviews that "focus on producing codable responses to the questions" may elicit better data than scaling and yes/no questions (Presser et al., 2004, p. 3). Consideration towards identifying problems and measurement error, the research and theory roles in setting a direction to identify mistakes, and aggregating and storing data to increase the body of knowledge (Presser et al., 2004) were factors while constructing a final survey for distribution.

Data Collection

Quantitative

Distribution and collection of correlational non-experimental data were via an electronic survey instrument after approval was obtained from Dakota State University's (DSU) Institutional Review Board (IRB), adhering to DSU's policy survey research (Approval #2020A70L-L). We invited survey participants from an available selection of viable IRDMs based on the current position, past positions, and familiarity with IR KSAs via social networking. Open-ended items were available via "other" fields that allow for free text writing and enable participants to add clarifying responses or additional selections that the researcher has not considered; this is constructive during pilot-testing and follow-up survey modifications. All other survey instrument questions will be restricted items with a "finite number of options provided by the researcher" (Privitera, 2018). These restricted items consisted of True/False, Yes/No, or Likert scale design to assist in coding with a limited number of points to record.

Qualitative

Loosely structured questions toward the end of the survey, combined with quantitative results, constitutes the qualitative portion of this explanatory concurrent research design

(Buckley, 2015). The salient points from which we derived the qualitative questions are reliant on the quantitative survey instrument concurrently. This concurrence exists in the final few items where the respondent may elaborate on their current choice, in an open-ended format (QUAN + qual) (John W Creswell, 2014, p. 279; John W. Creswell & Plano Clark, 2007, p. 119).

Data Analysis

Mixed methods, data collection, and analysis techniques occur at two points in this study (John W. Creswell & Plano Clark, 2007):

Quantitative: Data received underwent multiple steps during the analytical process. The sampling size includes success, failed, and unresponsive returns that are a factor in response bias. A two-tailed independent t-test (Kim, 2015) determines a statistically significant mean difference in efficacy between one or more commercial IR certifications and a statistically significant mean difference in whether hiring managers using certifications represent effective IR performance PQN-1 and PQN-2.

Qualitative: The researcher connected and explained results from the quantitative phase, exploring data for any unique, unexpected, contradictory, or surprising results for later integration (John W. Creswell & Plano Clark, 2007). The researcher utilized data analysis software to code, contextualize, and correlate data collections to organize and research information gathered (John W Creswell, 2014) in PQL-1.

Threats to Validity

This concurrent mixed methodology design research study does not contain an experimental component in which the researcher may control, modify, or predict variables. Therefore, this study is non-experimental, requiring validity instead of external factors; also, with non-experimental research, the outcomes can be generalized to a larger population (John W Creswell, 2014). Table 6 details Creswell's threats and responses pertinent to this study, as well as factors for consideration based on the IRDM skillset needs, moderately low population size (20-30), and time consideration for finding well situated and qualified participants:

TABLE 6 TYPES OF THREATS TO EXTERNAL VALIDITY

Types of Threats to External Validity	**Description of Threat**	**In Response, Actions the Researcher Can Take**
Interaction of selection and treatment	Because of the narrow characteristics of participants in the experiment, the researcher cannot generalize to individuals who do not have the characteristics of participants.	The researcher restricts claims to which the results cannot be generalized. The researcher conducts additional experiments with groups with different characteristics.
Interaction and setting and treatment	Because of the characteristics of the participants' setting in an experiment, a researcher cannot generalize to individuals in other settings.	The researcher needs to conduct additional experiments in the new settings to see if the same results occur as in the initial setting.
Interaction of history and treatment	Because results of an experiment are time-bound, a researcher cannot generalize the results to past or future situations.	The researcher needs to replicate the study at later times to determine if the same results occur as in the earlier time.

Reprinted from *Research design: Qualitative, quantitative, and mixed methods approaches (4th ed.)*, by Creswell, J. W.

Issues of Trustworthiness

Ensuring trust between participants and the researcher is essential to build and maintain truthful, valid, and objective answers to queries. No part of data collection and analysis utilized the participant's real identity as a component within the study. The role information is used only to validate the IRDM qualification to the researcher as a qualifier question.

Ethical procedures that followed as a part of this study were based on training and understanding of the code of ethics for researchers while working with human subjects, as per

DSU's IRB requirements, and detailed in an IRB application and approval process before participant interaction. The survey instrument denotes the purpose, benefits (if any), and participants' expectations, provide instructions, and notices that the survey is voluntary and termination instructions.

Chapter Summary

The research methodology presented in this chapter is based on a non-experimental, explanatory concurrent mixed methods design to examine the efficacy of commercial cybersecurity certifications for incident responders. The knowledge goals to be sought through this study are:

- Whether this method is usable and useful in garnering real-world performance of IR analyst?
- Whether this method was usable and useful in measuring and calculating IRDM input?
- Whether this method was usable and useful in assessing an IR analyst's practical abilities?

This chapter discusses the support of the goals above, survey instrumentation and participant selection, and sample size. Also covered were the data collection and analysis techniques employed to include threats to validity and trustworthiness issues.

This study's goals were to provide rigorous, measured, research-driven data to an organization in identifying whether commercial IR certification(s) is a useful instrument in selecting capable information security analysts. The selection would be for an organization seeking to employ, contract, or retain services required in meeting incident management requirements.

Chapter 4: Results and Findings

This chapter contains the results of the descriptive concurrent mixed methods study. Findings for multiple-choice questions that allowed for elaboration (SQL-1 through SQL-5) also follow the results segment.

Results

The researcher collected survey data to answer the following quantitative primary questions:

- **PQN1**: Is a candidate with an incident response specific certification preferred when hiring/recruiting?
- **PQN2**: Can organizations benefit from IR certified candidates to update, modify, and improve the IR process?

This section includes supporting data results for Table 3 Secondary Queries as ancillary support data. According to Table 7, top-level management stood at one-fifth (n=16) of all responses. Those in a managerial positional represented nearly half (n=40) of all answers. Non-managerial positions had a slightly higher response rate.

TABLE 7 JOB ROLES (SQN-1)

Job Roles	*n*	*%*
Top-Level Management/ Administrative level	16	20%
Departmental / Branch Manager	7	9%
Supervisory / Operative Manager	17	21%
Technical Lead	17	21%
Analyst	15	18%
HR / IT Recruiter	2	2%
Owner	1	1%
Other	7	8%
Total	82	100.00%

More than 80% of the sample was familiar with the following certifications: CEH, Network+, and Security+ (n>=61, >=83%). The majority of respondents (n>=42, >=51%) were acquainted with two-thirds of the certifications shown in Figure 4 (Full data table in Appendix D).

FIGURE 4 FAMILIARITY WITH SPECIFIC CERTIFICATIONS (SQN-2)

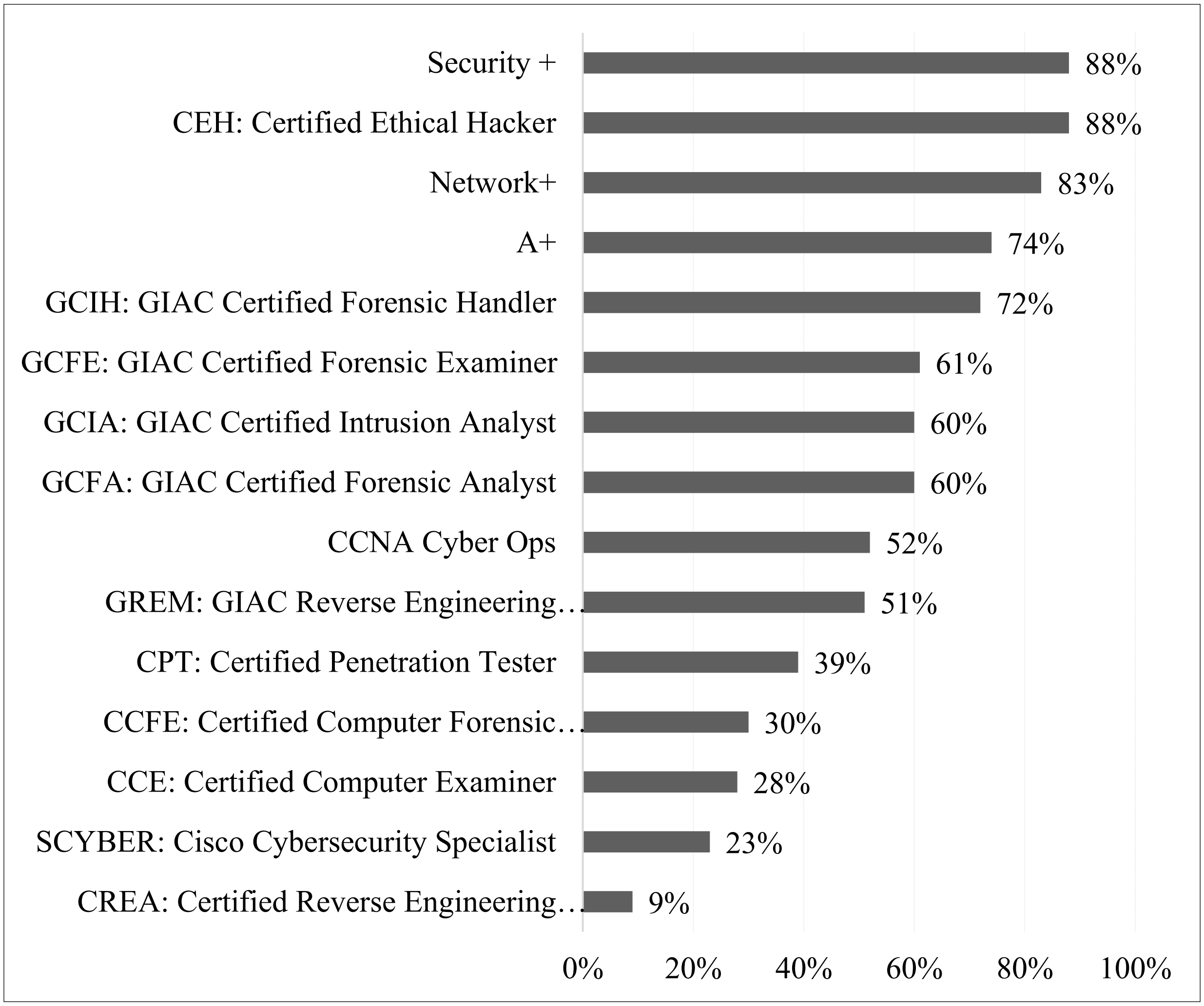


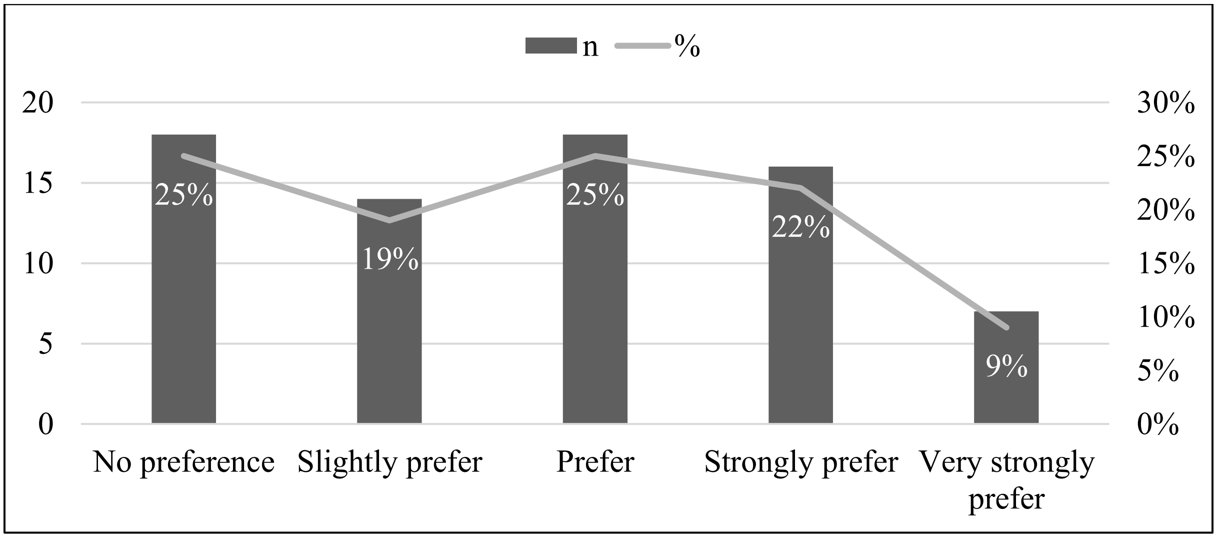
Table 8 shows how often the sample population checks whether the candidate holds an incident response related certification (n=44, 60%). Only 21% check sometimes, and 19% rarely or never check for certification.

TABLE 8 FREQUENCY OF CHECKING CANDIDATES' CERTIFICATION (SQN-3)

Check Candidates' Certification	*n*	*%*
Never	5	7%
Rarely	9	12%
Sometimes	15	21%
Quite Often	27	37%
Very Often	17	23%
Total	73	100%

More than half of the sample (n=41, 56%) preferred hiring candidates with incident response related certifications based on results in Figure 5. The total sample population was seventy-three; see Appendix E for the full table.

FIGURE 5 PREFER HIRING CANDIDATES WITH CERTIFICATION (PQN-1)



Sampling data from Table 9 shows IR certification helps to hire mostly through verification of candidates working towards exploring IR concepts (n=62, 85%), as a tiebreaker between candidates (65%), and used to simplify the vetting process (65%). More than half of the sample (57%) believe that IR certification verifies the knowledge base for IR and justifies the candidate's selection. A low 26% of the sample population believe a certification demonstrates the ability to perform the job.

TABLE 9 WAYS IR CERTIFICATION CAN ASSIST IN THE HIRING PROCESS (SQN-4)

Ways IR Certification Assists in Hiring Process	*Definitely Not*	*Probably Not*	*Neutral*	*Probably Yes*	*Definitely Yes*
	n (%)	n (%)	n (%)	n (%)	n (%)
Simplifies the vetting	8 (11%)	8 (11%)	10 (14%)	40 (55%)	7 (10%)
Verifies knowledge base of IR	5 (7%)	12 (16%)	14 (19%)	36 (49%)	6 (8%)
Verifies ability to perform IR job	7 (10%)	25 (34%)	22 (30%)	18 (25%)	1(1%)
Provides justification in choice	5 (7%)	10 (14%)	17 (23%)	34 (46%)	7 (10%)
Verifies effort to study IR concepts	3 (4%)	3 (4%)	5 (7%)	39 (53%)	23 (32%)
Acts as tiebreaker if pool is equal	3 (4%)	6 (8%)	17 (23%)	28 (39%)	19 (26%)

An overwhelming majority from Table 10 (n=60, 82%) believe certifications not specifically in the IR domain (e.g., networking, programming, system administration) are useful in increasing the effectiveness of an incident response certification.

TABLE 10 POTENTIAL USEFULNESS OF CERTIFICATIONS NOT IN IR DOMAIN (SQN-5)

The usefulness of other Certifications	*n*	*%*
Useless	1	1%
Probably useless	2	3%
Neutral	10	14%
Probably useful	27	37%
Useful	33	45%
Total	73	100%

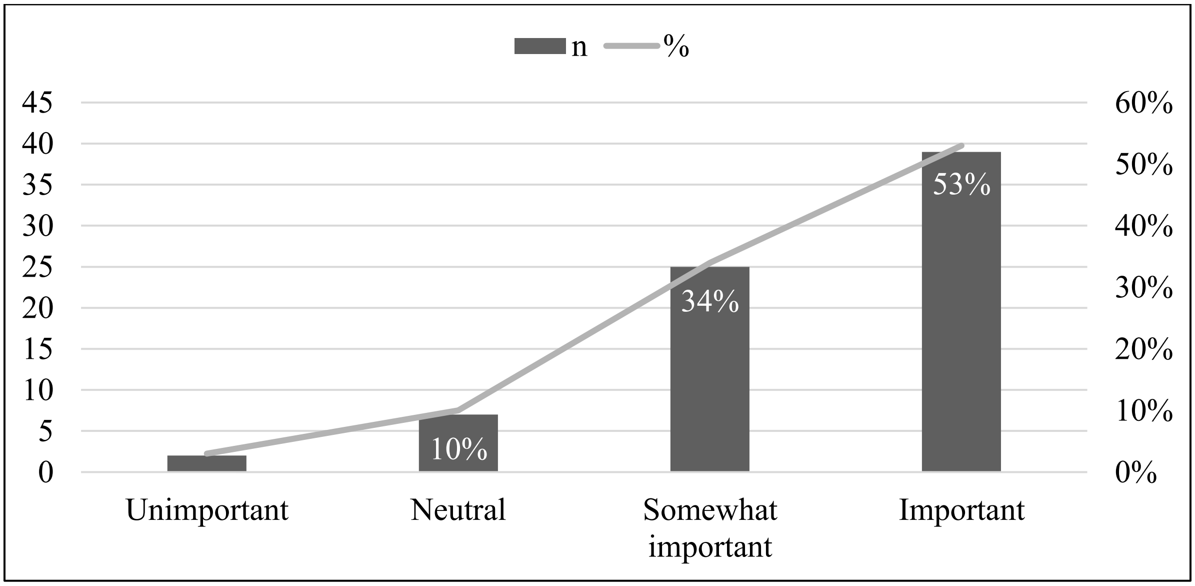
Table 11 presents three influencers to certification value. For most respondents (n=41, 53%), the method of an incident response certification test, such as in-person, online, or proctored vs. non-proctored, is a factor when forming an opinion about the value of the certification. Nearly three-fifths of the sample (59%) state the influence of marketing (e.g., brand recognition, history of certification) impacts the incident response certification value.

TABLE 11 POTENTIAL INFLUENCE ON THE VALUE OF CERTIFICATION (SQN-6)

Influencers	*Definitely Not*	*Probably Not*	*Neutral*	*Probably Yes*	*Definitely Yes*
	n (%)	n (%)	n (%)	n (%)	n (%)
Method of IR certification test given	7 (10%)	11 (15%)	16 (22%)	21 (29%)	18(24%)
Marketing (brand recognition, history)	4 (6%)	11 (15%)	15 (20%)	29 (40%)	14 (19%)
Job market in the region	5 (7%)	9 (12%)	9 (12%)	33 (45%)	17(23%)

Sampling data in Figure 6 shows that the inclusion of a practical component while earning an IR certification is important for 87% of the sample population (n=64).

FIGURE 6 IMPORTANCE OF A PRACTICAL COMPONENT (SQN-7)



According to the results in Table 12, vendor-neutral certifications (n=39) held higher importance than vendor-specific certifications (n=33). A large percentage of the sample (75%) believe vendor-specific certifications are neutral or only somewhat important (35% each).

TABLE 12 IMPORTANCE OF VENDOR-SPECIFIC AND VENDOR NON -SPECIFIC CERTIFICATIONS (SQN-8)

Importance of Vendor Certifications	*Vendor-Specific*		*Vendor-Neutral*	
	n	*%*	*n*	*%*
Unimportant	6	8%	3	4%
Somewhat unimportant	8	11%	1	1%
Neutral	26	35%	20	27%
Somewhat important	26	35%	26	36%
Important	7	10%	23	32%
Total	73	100%	73	100%

Survey takers overwhelmingly (n=71) stated that all certifications are not equal, and some are harder than others based on Table 13.

TABLE 13 VARYING DIFFICULTY OF IR RESPONSE CERTIFICATIONS (SQN-9)

Some More Difficult than Others?	*n*	*%*
Yes	71	97%
No	2	3%
Total	73	100%

Table 14 only represents respondents claiming knowledge of one or more certifications, as shown in Figure 4 Familiarity with Specific Certifications (SQN-2), based on the survey instrument's logic flow. Resultant data show that CEH, A+, Network+, and Security+ were the easiest certifications (n>=47), while GREM stood out as the hardest (n=44). CCE was the most obscure (n=27), while CEH, A+, Network+, and Security+ were most familiar (n>=61), according to Table 14.

Table 14 Level of Difficulty for Certifications (SQN-10)

Level of Difficulty	*Novice* n (%)	*Intermediate* n (%)	*Advanced* n (%)	*Total* n (%)
CCE: Certified Computer Examiner	9 (33%)	15 (56%)	3 11%)	27 (100%)
CEH: Certified Ethical Hacker	47 (73%)	14 (22%)	3 (5%)	64 (100%)
GCFE: GIAC Certified Forensic Examiner	3 (5%)	35 (64%)	17 (31%)	55 (100%)
GCFA: GIAC Certified Forensic Analyst	8(15%)	25(47%)	20 (38%)	53 (100%)
GCIH: GIAC Certified Forensic Handler	14 (25%)	36 (63%)	7 (12%)	57 (100%)
GCIA: GIAC Certified Intrusion Analyst	8 (16%)	30 (59%)	13 (25%)	51 (100%)
GREM: GIAC Reverse Engineering Malware	1 (2%)	9 (17%)	44 (81%)	54 (100%)
CCFE: Certified Computer Forensic Examiner	2 (5%)	26 (65%)	12 (30%)	40 (100%)
CPT: Certified Penetration Tester	8 (22%)	19 (51%)	10 (27%)	37 (100%)
CREA: Certified Reverse Engineering Analyst	2 (7%)	10 (34%)	17(59%2)	29 (100%)
SCYBER: Cisco Cybersecurity Specialist	7 (23%)	21 (70%)	2 (7%)	30 (100%)
CCNA Cyber Ops	12 (29%)	22 (54%)	7 (17%)	41 (100%)
A+	57 (93%)	3 (5%)	1 (2%)	61 (100%)
Network+	62 (95%)	2 (3%)	1 (2%)	65 (100%)
Security+	55 (82%)	11 (16%)	1 (2%)	67 100%)

Based on Figure 7, IR certifications are likely to assist a candidate in communication within the IR realm from a technical standpoint (n=55, 87%) and provide an immediate contribution to the IR effort (n=44, 70%). Fifty-nine percent of the sample population believe IR certifications may help a candidate update, modify, and improve the IR process (n=37, 59%) and respond to incidents (n=39, 53%). There was a low number of respondents who saw leadership (n=18, 28%), employee replacement (n=25, 40%), or contributions to training (n=27, 43%) as benefits of obtaining an IR certification (full table in Appendix D).

Figure 7 Benefits of Hiring IR Certified Job Candidate (PQN-2)

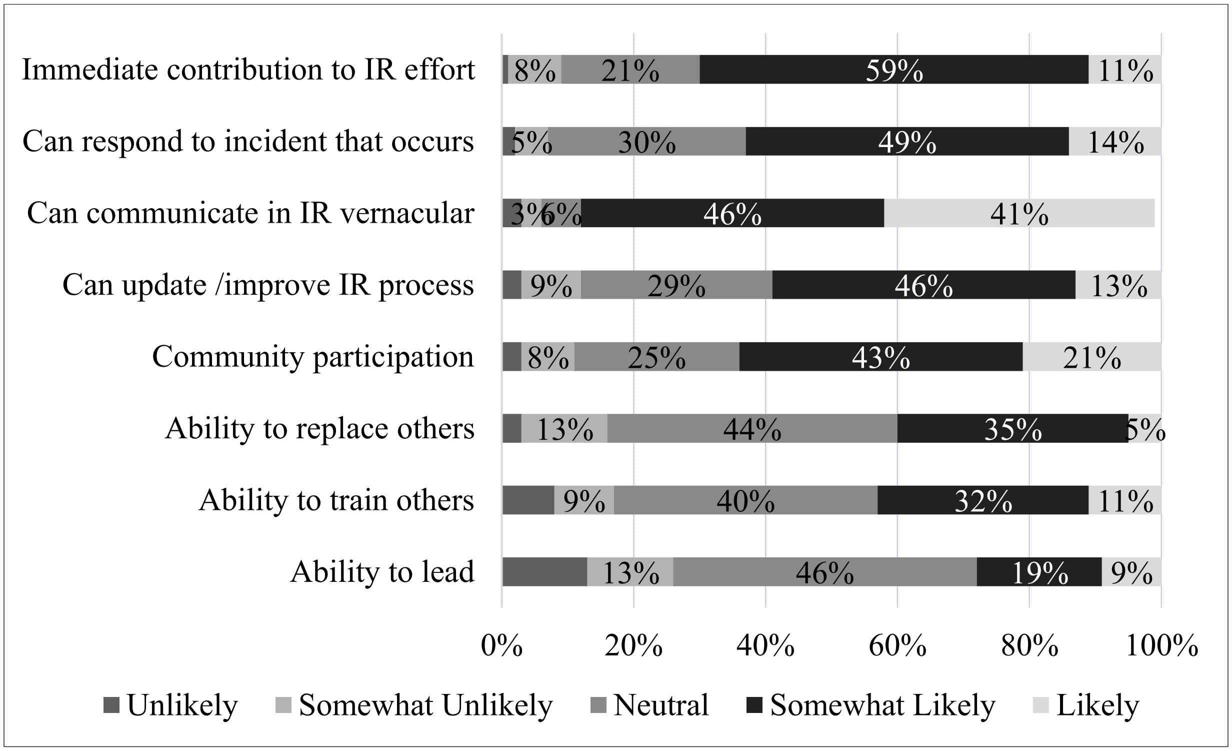


Table 15 shows (n=46) survey takers believe those candidates who already have several years of experience in incident response may still benefit from a related certification.

Table 15 Potential Benefit of IR Certification for Long Term IR Persons (SQN-11)

Beneficial to Long Term Employees?	*n*	*%*
Definitely not	--	--
Probably not	14	22%
Neutral	4	6%
Probably yes	35	56%
Definitely yes	10	16%
Total	63	100%

According to experienced individuals mentioned in previous Table 15, more than four-fifths of respondents (n=51, 81%) received value from incident response certifications employees (n=41) complete after being hired based on Table 16.

TABLE 16 POTENTIAL BENEFIT TO ORGANIZATION (SQN-12)

Beneficial to Organization?	*n*	*%*
Definitely not	--	--
Probably not	4	6%
Neutral	8	13%
Probably yes	35	56%
Definitely yes	16	25%
Total	63	100%

An overwhelming number of respondents (n=53) from Table 17 recommend one or more incident response certifications to candidates or employees. The researcher or respondent did not include certification suggestions within the survey instrument.

TABLE 17 LIKELIHOOD OF RECOMMENDING IR CERTIFICATION TO CANDIDATE/ EMPLOYEE (SQN-13)

Likelihood	*n*	*%*
Unlikely	--	--
Somewhat unlikely	4	6%
Neutral	6	9%
Somewhat likely	30	48%
Likely	23	37%
Total	63	100%

Derived from Figure 5 Prefer Hiring Candidates With Certification (PQN-1), Table 18 further classifies the results between managers (n=37) and non-managers (n=36). Independent T-tests find statistically significant differences in these two areas of PQN-1 and PQN-2. For PQN-

1, the variances are equal in both groups with an F statistic=.00, T value=2.42, and p=.02. Both groups prefer hiring candidates with an IR certification (df=71), though managers (M=3.08) more strongly than non-managers (M=2.36).

TABLE 18 DIFFERENCE BETWEEN MANAGERS AND NON-MANAGERS

Survey Question	*Group*	*N*	*M*	*SD*
Prefers hiring candidates with IR certification (PQN-1)	Managers	37	3.08	1.30
	Non-Managers	36	2.36	1.25
Believes IR certified job candidates can update, modify, improve the IR process (PQN-2)	Managers	31	3.87	.88
	Non-Managers	32	3.25	.92

Survey Question	*F statistic*	*p for F*	*t value*	*df*	*p*
Prefers hiring candidates with IR certification (PQN-1)	.00	.99	2.42	71	.02*
Believes IR certified candidates can update, modify, improve the IR process (PQN-2)	.27	.60	2.74	61	.00**

**p<.05*

***p<.01*

PQN-2 testing results stem from [s]. Both managers (n=31) and non-managers (n=32) believe IR certified job candidates can improve the IR process with t-value=2.74 and only a four-hundredths difference in SD between them.

Findings

The researcher collected survey data to answer the following qualitative primary question:

- **PQL1**: What skills, knowledge, and abilities (KSA's) do you believe an effective incident responder should possess?

This section also includes supporting data results for Table 3 Secondary Queries (SQL-1 through SQL-5).

According to Table 19, more than 90% (n=59) believe skills outside of the incident response domain enable a more effective responder. More than half of the respondents (n=39) believe obtaining IR certifications can help identify those skills are present.

TABLE 19 NON-IR SKILLS THAT MAY ASSIST A RESPONDER (SQL-1)

Are other skills necessary to be an effective incident responder; if so, can IR certifications help?	*n*	*%*
No, outside skills are not necessary.	3	4.8%
Yes, outside skills are necessary, but certifications do not help	20	32.3%
Yes, outside skills are necessary. Yes, certifications help	39	62.9%
Total	62	100.0%

A smaller population (n=19) elaborated on which skills are necessary for an incident responder (see SQL-1 Word Frequencyin Appendix E), with the following results in Table 20 for c>=3:

TABLE 20 SQL-1 WORD FREQUENCY

Word	*Count (c)*	*Weighted Percentage (%)*	*Similar Words*
networking	7	10.94	network, networking
analysis	4	6.25	analysis
on-the-job training	3	4.69	OJT
operating	3	4.69	operating
programming	3	4.69	programming
sysadmin	3	4.69	sysadmin
system	3	4.69	system, systems

Nearly two-thirds (n=41) of all responses (n=62) state that response operating procedures are needed, and certifications can assist with this task, according to Table 21.

TABLE 21 ASSIST IN IR PROCESSES (SQL-2)

SOP's necessary for responder effectiveness; if so, can IR certifications help?	*n*	*%*
No, SOP creation is not necessary to be an effective incident responder.	4	6.5%
Yes, SOP creation is necessary to be an effective incident responder, but certifications do not help	17	27.4%
Yes, SOP creation is necessary to be an effective incident responder, and certifications can help	41	66.1%
Total	62	100.0%

The most common theme amongst the few respondents (n=4) who chose to elaborate on SQL-2 was exposure to incident response procedures and best practices while undergoing certification training.

Table 22 shows that most respondents (n=61) agree that an analytical mindset makes for a more effective responder; more than half (n=34) believe certifications support this approach.

TABLE 22 ANALYTICAL MINDSET (SQL-3)

If an analytical mindset needed for responder effectiveness, can IR certifications help?	*n*	*%*
No, an analytical mindset is not necessary to be an effective incident responder.	1	1.6%
Yes, an analytical mindset is necessary to be an effective incident responder, but certifications cannot help	27	43.5%
Yes, an analytical mindset is necessary to be an effective incident responder, and certifications can help	34	54.8%
Total	62	100.0%

The only theme to arise from additional comments (n=5) toward SQL-3 is that certification may increase the analysts' reasoning ability due to exposure to various situations covered in material and testing.

A large majority (n=55) of the sample provides the same training level to their IR staff regardless of earning a certification, according to Table 23.

TABLE 23 TRAINING EQUALITY (SQL-4)

New responders receive the same amount of training regardless of earning a certification?	*n*	*%*
Yes, all incident responders receive the same training regardless of any IR certifications they may hold.	55	88.7%
No, incident responders with IR certifications receive less training.	7	11.3%
Total	62	100.0%

For those that expounded on SQL-4 (n=5), the central theme was training is based on the organization and its needs; therefore, the certification has no bearing.

Data coding results relating to the question of which skills, knowledge, and abilities (KSA's) an IRDM believes an effective incident responder should possess (PQL-1) produced the following results in Table 24. See PQL-1 Full Word Coding in Appendix E for the full listing.

TABLE 24 PQL-1 WORD CODING

Cluster 1: Analysis	*Cluster 2: Data*	*Cluster 3: Critical Thinking*	*Cluster 4: Awareness*
• network analysis (9) • malware analysis (5) • data analysis (4) • memory analysis (3) • technical analysis (1)	• data analysis (4) • data science (2) • data sensitivity (1)	• critical thinking (6)	• enterprise awareness (3) • business awareness (1) • situational awareness (1)

Coupled with the top-ten word frequencies in Table 25 (see PQL-1 Word Frequency in Appendix E for the full listing), the high-three emerging themes (c>=19) based on descending order were networking, the multiple forms of analysis (network, malware, data, and memory), and communication. One soft-skill mentioned frequently enough to reside in the top-ten was enthusiasm (c=9).

TABLE 25 PQL-1 WORD FREQUENCY

Word	Count	Weighted Percentage (%)	Similar Words
networking	23	7.03	network, networking
analysis	22	6.73	analysis
communication	19	5.50	communication, communications
analytical	11	3.36	analytic, analytical
procedure	11	3.36	procedure
enthusiasm	9	2.75	enthusiasm, enthusiasm
chain	7	2.14	kill chain
critical	7	2.14	critical
data	7	2.14	data
forensics	7	2.14	forensics

Chapter Summary

This results and findings chapter highlighted the data points collected via a twenty-six-question survey instrument detailed in Appendix C. The chapter required a results and findings section for quantitative and qualitative data points due to the mixed-methods design.

The results section highlights the primary questions (PQN-1/2) and iterates through each supporting question (SQN-1 through SQN-13). Development of PQN-1 comes from Figure 5 Prefer Hiring Candidates With Certification (PQN-1). Managers and non-managers represent two distinct groups for which the primary statistics were calculated and presented.

The findings section provides coding and frequency results supporting the primary qualitative question PQL-1, and five ancillary questions (SQL-1 through SQL-5). Word frequency analysis was performed by statistical software on PQL-1 and SQL-1 due to the amount of textual data. SQL-2 through SQL-5 did not require computing resources, as those respondents that chose to elaborate were of a small enough quantity allowing data dissemination by sight.

Chapter 5: Conclusions, Interpretations, and Recommendations

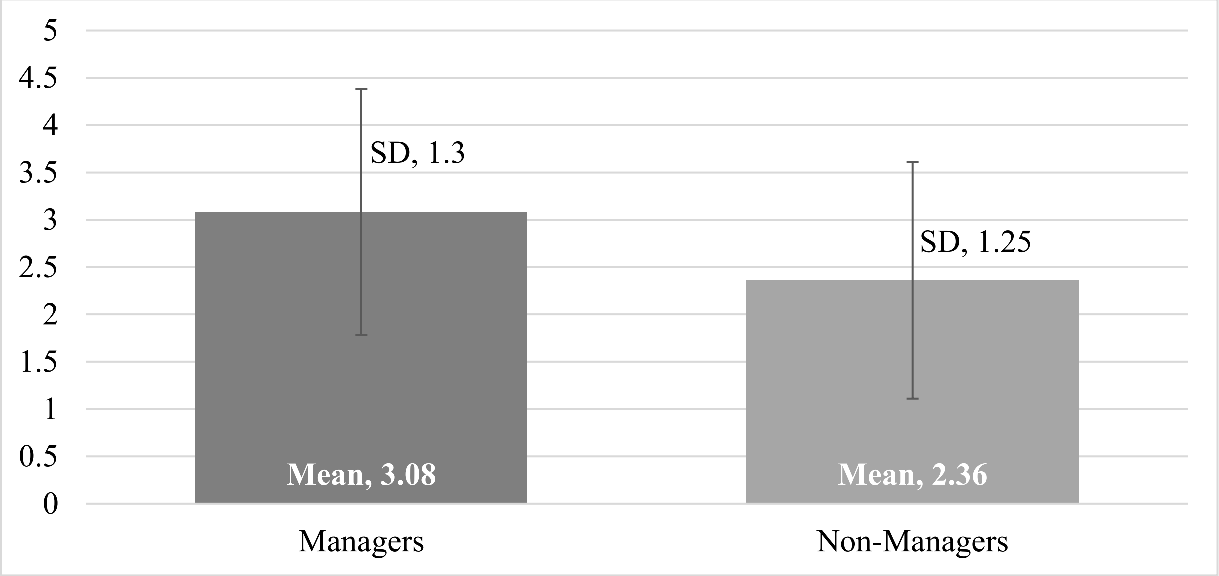
The purpose of this study is to determine whether one or more incident response certifications are viable credentials toward hiring decisions. The problem was the lack of academic research that may help the hiring entity choose an effective candidate. This research study applied an explanatory concurrent mixed methods design, collecting quantitative and qualitative data in parallel. Data collection was a single survey instrument per DSU's IRB requirements met before participant interaction. The components of this study: literature review, methodology, accompanying survey, and subsequent analysis, support the hypothesis through the three research questions. This study's hypothesis is: Can commercially available incident response cybersecurity certifications be a useful criterion for selecting preliminary incident response (IR) candidate by a hiring entity. The null hypothesis is that a hiring entity does not prefer hiring candidates with an IR certification. The questions supporting the hypothesis are:

- PQN-1: Is a candidate with an incident response specific certification preferred when hiring/recruiting?
- PQN-2: Can organizations benefit from IR certified candidates to update, modify, and improve the IR process?
- PQL-1: What skills, knowledge, and abilities (KSA's) do you believe an effective incident responder should possess?

Conclusions

A literature review to support or oppose IR certification preference during candidate selection (PQN-1), while not relating specifically to IR, did favor hiring IT certificate holding candidates. On a scale of one to five, one being no preference, and five very strongly preferring, this study found that managers prefer (M=3.08), and non-managers only slightly prefer (M=2.36) hiring candidates with IR certification(s) as shown in Figure 8. Manager and non-manager respondents were very nearly equal (N=37 vs. N=36) in the sample population size for this study.

FIGURE 8 MEAN: PREFERENCE FOR IR CERTIFICATION HIRING (PQN-1)

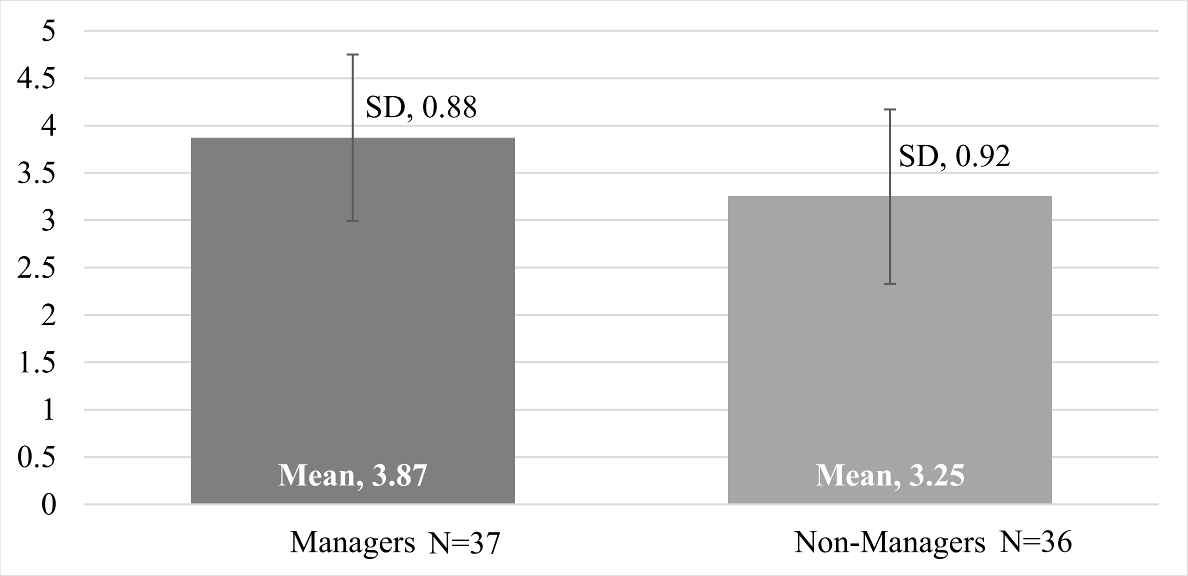


Bartlett’s 2002 study found a strong correlation between IT certification holders and recruitment ease (Bartlett, 2002, pp. 63-66). There is a correlation with some of this study's results in that more extensive, broader perspective of information technology. More than half of respondents use IR certifications in the hiring process to simplify the vetting of applicants and tie-breaking considerations (Table 9, SQN-4). While Cegielski’s study pointed out that IT certification did not correlate with aptitude (Cegielski, 2004, p. 105), only 26% of this study's respondents believed commercial accreditations verified the ability to perform the IR job (Table 9, SQN-4).

Pierce’s 2009 study noted the certification process's hindrance while also being relevant in the [IT] field (Pierce, 2009, p. 159). The field's relevance should be represented in the myriad of testing processes, varying based on certification type (CompTIA, 2020) and vendor offerings. Gleghorn & Gordon’s study indicated that vendor-specific and vendor-neutral certifications might play a role in the initial hiring of a prospective responder (Gleghorn & Gordon, 2012, p. 16). For incident response certifications, vendor-neutral certifications were more important (68%) than vendor-specific (45%). The sample population communicated the importance of a practical component (87% of this study's response) within the IR certification process (Figure 6, SQN-7).

The 70% likelihood for immediate contribution to the IR effort (Figure 7 Benefits of Hiring IR Certified Job Candidate (PQN-2)), coupled with the mean results of whether IR certified job candidates could update, modify, or improve the IR process in Figure 9 below, indicates there are relevant benefits to hiring IR certified job candidates.

FIGURE 9 MEAN: BELIEVE IR CERTIFIED JOB CANDIDATES CAN UPDATE, MODIFY, IMPROVE THE IR PROCESS (PQN-2)



This contribution would assist with the labor statistics double-digit growth outlook of Information Security Analysts in the next five years (*U.S. Bureau of Labor Statistics, Employment Projections program*, 2019). The data reflects the correlation of contribution in operational procedure creation, where 66% of respondents believe SOP's are needed and certifications can assist in this process based on exposure to best practices (Table 21 Assist in IR processes (SQL-2)), an essential skillset for a defender (Killcrece et al., 2003, p. 135).

Network+ is in the top three certifications participants were familiar with based on Figure 4 Familiarity with Specific Certifications (SQN-2). The most significant and highest frequency word during qualitative analysis in this study is “network[ing]” (Table 24 PQL-1 Word Coding and Table 25 PQL-1 Word Frequency). The high usage of the word network[ing] correlates with Network+ being one of the requirements for meeting qualifications for a CND-IR within DoD’s 8570.01M manual (Poe, 2018). Along the same line, fundamental networking knowledge for incident responders is the first Knowledge Objective (see Knowledge in Appendix A) in the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (Newhouse et al., 2017). Ninety-five percent of respondents ranked Network+ as a novice level of difficulty in Table 14 Level of Difficulty for Certifications (SQN-10).

Querying for soft skills, such as communication and problem-solving (Crumpler & Lewis, 2019) relating to IR certifications and hiring, was not explicitly part of the survey instrument. These soft skills became apparent in the data while disseminating results. Risk awareness and communication are essential for incident response teams (Ramilli, 2018), reflected in quantitative questioning as a cluster of awareness in Table 24 PQL-1 Word Coding and communications as the third-highest mention in Table 25 PQL-1 Word Frequency. Critical thinking and enthusiasm are notably absent in the NICE framework but find a place in Table 25 as one of the top-ten frequent words. Tangentially related are problem-solving skills within an analytic mindset (Zyphur, 2009, p. 678), which, based on Table 22 Analytical mindset (SQL-3), did not provide substantial support (54.8%) towards asserting IR certifications can assist in improving that skill.

Interpretations

This study aimed to determine whether a commercial IR certification is a useful instrument in selecting adept information security analysts. Organizations seeking to employ, contract, or retain services required to meet incident management requirements may benefit from this study's results. While the data does suggest a candidate with an incident response certification is preferred, the results show preference at mild and low significance for managers and non-managers, respectively (PQN-1). Unsurprisingly, the most considerable contribution is leveraging the pertinent jargon in the IR domain (PQN-2). The ability to communicate, both written and orally, during a cyber incident would contribute to the response process as a shared vernacular is a logical first step in building a foundation for further education and involvement. Not mentioned as IR components for certification are team building, shared trust, or team knowledge, but they are factors in other successful responder teams such as medicine, military, and nuclear power (Steinke et al., 2015, pp. 23-25). Perhaps the efficacy of these cybersecurity analysis credentials can be further bolstered by incorporating additional elements that influence other teams.

It is apparent from the data that certifications simplify the candidate pool vetting process and justify the selection choice for the IRDM. There is a clear distinction between knowledge and ability. The majority of the sample believe certifications verify knowledge but not the ability to perform the job (Table 9 Ways IR Certification Can Assist in the Hiring Process (SQN-4)). This result coincides with the overwhelming importance of practical components within a certification (Figure 6 Importance Of A Practical Component (SQN-7)) that may assist in honing IR abilities.

Certified Ethical Hacking tied with Security+ as having the highest level of familiarity. Analysis, along with its word variants, were top terms in the qualitative portion of data. It is notable that offensive skills, such as penetration testing, exploitation, and offensive methodologies, were not mentioned often as examples of additional certifications or KSA's desired by IRDM's. NICE's Cybersecurity Workforce Framework has dedicated roles for Exploitation, Vulnerability, Research, and Development, as well as Cyber Operation (Newhouse et al., 2017, pp. 11-23); all of which involve attack and exploitation. The KSA's (Appendix A) for the NICE Incident Response (CIR) role offers familiarity with offensive processes. Knowledge of offense is required to defend, but the capability indicators at the intermediate and advanced levels declare penetration testing as needed experience. The lack of mentioning offensive skills within entry-level IR and capability indicators suggest offense and corresponding certifications that cover this topic are either out-of-scope for newer defenders, or while familial to the survey respondents, offense not necessary from a defensive posture. There may be a relation to the high importance placed on the inclusion of a practical component to certification (SQN-7), where exploitation and testing are hands-on activities that require lab environments and resources outside the scope of an entry-level certification. Further research in recommendations and future work sections that follow expand on this premise.

Networking is of high importance to IRDM's, followed closely by multiple analysis paths (network, malware, data, and memory). All but one of the sample population agree an analytical mindset is necessary for responder effectiveness (Table 22 Analytical mindset (SQL-3)). There was an 11.3% difference between those believing certifications can help in this regard and those that do not. The magnitude of that difference is not significant enough to conclude certifications can foster or improve a candidate's analytical mindset.

Recommendations

The IT domain is vast, and individuals' components and fields within IT intersect each other, including skillsets, expertise, and practical knowledge to support multiple roles. Incident response is unique in that a hands-on, analytical mindset and situational awareness is required to excel in the position. Incident response is inherently a reactive process. Based on adversarial actions [and intent], there exists a real challenge for the modern IR practitioner to learn needed deterrence, techniques, tactics, and procedures in a certification process alone as they are continually evolving with the cyber terrain, potential vulnerabilities, and exploit vectors (Iasiello, 2014, pp. 53,67). Possible coupling with on-the-job experience, formal academic instruction that focuses on core fundamentals, and mastery of foundational TTP's over a more extended period, as opposed to the short boot-camp-style instruction many certification courses employ. This increased time may assist in the retention and practical usage of learned information. With a minimum number of hours working in a realistic environment, the on-job-experience may foster the team dynamic absent from introductory IR certifications.

Additional conclusions may be drawn within a particular field as IR by a longitudinal study to isolate the parameters that constitute a practical certification for the domain (Goldblatt, 1996). Determining the ideal permutation of experience(s), certification(s), and formal education that establishes a concrete incident responder from the human capital perspective (Evans & Reeder, 2010) could add substantial evidence to support or repudiate the certification efficacy question within the IR realm.

Future Works

It is clear from this research that certifications influence hiring decisions, despite how effective the result. How does that compare to job experience, enthusiasm, potential, academic achievements, and study curriculum?

Incident responders' roles exist across many disciplines, such as fire control, law enforcement, hazardous materials handling, emergency management, and medicine. The commonality between cyber IR and other IR variations in response management involves leveraging all available resources to meet the objectives (Chen & Sharma, 2012, p. 3). By harnessing capabilities, an IR team can achieve functional competency and maximize an effective and satisfactory response (Chen & Sharma, 2012, p. 1). Emergency medical teams must collaborate to adapt to changing patient needs. Military response teams must quickly communicate with team members while altering mission demands. Nuclear power plant operators must make decisions based on complicated systems and communicate effectively (Steinke et al., 2015). Cyber incident response is not without the need of any of the abilities mentioned above, and future research can focus on the components and corollaries within external incident response systems to incorporate into certification curricula.

The many facets of knowledge, skills, and abilities in IR, coupled with the high-level tasks defined in the NICE Framework (Newhouse et al., 2017), have relevance to candidate hiring, retention, and performance for this field of expertise. Utilizing a more detailed questionnaire on a larger scale with performance evaluations, testing, and quizzes, along with candidate and individual observer interviews, may result in a compendium of additional usefulness about this topic. Further consideration should be toward certifications offered by institutes of higher learning and how they may re-enforce or influence hiring managers' opinions when coupled, or instead of, commercial certifications.

The following list represents possible queries toward a more extensive analysis that may incorporate detailed interviews and observations to capture increased introspection into the IR certification and hiring process:

- What magnitude of experience may be more valuable than a certification?
- Many believe certifications outside of IR to be valuable – specifically, which certifications fall in this category?
- Survey takers believe those who have experience in incident response may still benefit from a related certification. Which certifications would meet this criterion?
- Which certifications specifically increase abilities and not just knowledge, and do they have a practical component?
- How do certifications compare to more extended instruction periods, such as those provided in higher education institutes, or certifications that require a minimum number of proficiency hours?

Lastly, a single-case mechanism experiment in validation research utilizing Technical Action Research with the following implementation may yield valuable kinetic results that would be a corollary to this mixed-method study. A preliminary TAR study outline may represent the following:

Problem: Recruitment of analytically minded candidates that can fulfill the requirements of incident response is difficult. Frequently candidates possess the theoretical knowledge needed but lack the practical, analytical skills required to determine necessary steps to perform

Cybersecurity Framework's functions: identity, protect, detect, respond, and recover during an incident.

Objective: Develop a treatment for candidate recruitment that can determine the best fit for IR work.

Goal: Utilize a modular assessment framework in a simulated environment that assesses the candidate's ability to think through analytical scenarios and perform IR tasks. This framework would help learn the experimental artifact's effectiveness while still under development and not wholly transferred to the problem situation.

Each iteration of the artifacts can be studied on a case-by-case basis and aid the stakeholder. This research may be driven by [testing of] the artifact itself, not by the problem, thereby validating the experimental artifact. The treatment is the interaction between the artifact (for a practical purpose) and the problem context. Not just designing an artifact (two in this case) and developed the interaction between the artifact and the problem context, intended to treat the problem. Treatment would be an incident response analyst interacting with a simulated threat landscape environment to assess analytical capabilities for a real-world type of incident exploration and dissemination by the user.

References

(ISC)². (2018). Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens. *Cybersecurity Workforce Study.* Retrieved from https://www.isc2.org/-/media/7CC1598DE430469195F81017658B15D0.ashx

Adelman, C. (2000). *A Parallel Postsecondary Universe: The Certification Systemin Information Technology.* Office of Educational Research and Improvement, U.S. Dept. of Education. Retrieved from https://eric.ed.gov/?id=ED445246

Ahmad, A., Hadgkiss, J., & Ruighaver, A. B. (2012). Incident response teams – Challenges in supporting the organisational security function. *COMPUT SECUR, 31*(5), 643-652. doi:10.1016/j.cose.2012.04.001

Andrade, R. O., & Yoo, S. G. (2019). Cognitive security: A comprehensive study of cognitive science in cybersecurity. *Journal of Information Security and Applications, 48*, 102352.

Andres, R. (2012). The Emerging Structure of Strategic Cyber Offense, Cyber Defense, and Cyber Deterrence. *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, 89-104.

Bartlett, K. R. (2002). *The Perceived Influence of Industry-Sponsored Credentials in the Information Technology Industry.* University of Minnesota, St. Paul, MN. Retrieved from https://files.eric.ed.gov/fulltext/ED465072.pdf

Bartlett, K. R., Horwitz, S. K., Ipe, M., & Liu, Y. (2005). The Perceived Influence of Industry-Sponsored Credentials on the Recruitment Process in the Information Technology Industry: Employer and Employee Perspectives. *Journal of Career and Technical Education, 21*(2), 51-65. Retrieved from https://files.eric.ed.gov/fulltext/EJ1069519.pdf

Benslimane, Y., Yang, Z., & Bahli, B. (2016). *Information security between standards, certifications and technologies: An empirical study.* Paper presented at the 2016 International Conference on Information Science and Security (ICISS).

Buckley, A. P. (2015). Using Sequential Mixed Methods in Enterprise Policy Evaluation. *Special Mixed Methods Edition, 13*(November). doi:10.21427/D7MN57

CCNA Cyber Ops. (2020). Retrieved from https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/associate/ccna-cyber-ops.html

Cegielski, C. G. (2004). Who values technology certification? *Communications of the ACM, 47*(10), 103-105. doi:10.1145/1022594.1022627

Chen, R., & Sharma, S. K. (2012). Organizational capabilities in emergency incident response: An empirical examination. *Proceedings of the 7th Annual Midwest Association for Information (MWAIS) Green Bay, WI*. Atlanta, GA: Association for Information Systems (AIS).

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Special Publication 800-61 Revision 2: Computer security incident handling guide - Recommendations of the National Institute of Standards and Technology. doi:10.6028/NIST.SP.800-61r2

Cisco. (2016). *CCNA cyber ops certification program at-a-glance.* Retrieved from https://www.cisco.com/c/dam/en_us/training-events/certifications/associate/cyberops-associate-at-a-glance.pdf

Collins, D. (2003). Pretesting survey instruments: An overview of cognitive methods. *Quality of Life Research, 12*(3), 229-238. doi:10.1023/A:1023254226592

CompTIA. (2020). CompTIA Learning and Training. Retrieved from https://www.comptia.org/training

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). Thousand Oaks: Sage publications.

Creswell, J. W., & Plano Clark, V. L. (2007). *Designing and conducting mixed methods research*. Thousand Oaks, Calif.: Thousand Oaks, Calif. : SAGE Publications.

Crumpler, W., & Lewis, J. A. (2019). *Cybersecurity Workforce Gap*: Center for Strategic and International Studies (CSIS).

Cuncic, A. (2020). Understanding Internal and External Validity. Retrieved from https://www.verywellmind.com/internal-and-external-validity-4584479

Cyber Security Education. (2018). How to become an incident responder. Retrieved from https://www.cybersecurityeducation.org/careers/incident-responder/

Denzin, N. K. (1978). *The research act: A theoretical introduction to sociological methods* (2d ed.). New York: McGraw-Hill.

DoD. (2015). *Information Assurance Workforce Improvement Program*. (DoD 8570.01-M). Department of Defense Retrieved from https://iase.disa.mil/iawip/pages/index.aspx

Encyclopedia of Case Study Research. (2010). doi:10.4135/9781412957397

European Union Agency for Network and Information Security [ENISA]. (2018). *ENISA threat landscape report 2017: 15 top cyber-threats and trends.* Retrieved from https://doi.org/10.2824/967192

Evans, K., & Reeder, F. (2010). A human capital crisis in cybersecurity: Technical proficiency matters. 7.

Federal Trade Commission. (2019). *Consumer Sentinel Network Data Book 2019*. Federal Trade Commission Retrieved from https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2019

GIAC Certifications: Cyber Defense. (2020). Retrieved from https://www.giac.org/certifications/cyber-defense

Ginovsky, J. (2012). Cyber attacks are soaring. How to thwart them. *ABA Banking Journal, 104*(6), 22-25.

Gleghorn, G. D., & Gordon, J. (2012). A quantitative examination of perceived promotability of information security professionals with vendor-specific certifications versus vendor-neutral certifications. *Research in Business and Economics Journal, 6*, 1. Retrieved from https://search.proquest.com/docview/901925335/?pq-origsite=primo

Goldblatt, J. J. (1996). *Certification and Event Management: A Qualitative and Quantitative Approach to Assessment*, Ann Arbor.

Goldin, C. (2014). Human Capital. *Handbook of cliometrics*, 55-86.

Gonzalez, J. W. J. J., Kossakowski, K.-P., & Wiik, J. (2005). *Limits to effectiveness in computer security incident response teams.* Paper presented at the Boston, Massachusetts: Twenty Third International Conference of the System Dynamics Society.

Greene, J. C., Caracelli, V. J., & Graham, W. F. (1989). Toward a conceptual framework for mixed-method evaluation designs. *Educational evaluation and policy analysis, 11*(3), 255-274.

Grover, M., Reinicke, B., & Cummings, J. (2016). How secure is education in Information Technology? A method for evaluating security education in IT. *Information System Education Journal, 14*(3), 29-44. Retrieved from http://isedj.org/2016-14/n3/ISEDJv14n3p29.html

Hamill, T. A. (2019). The CITI Program. *Reproducibility of Research Results.* Retrieved from https://www.citiprogram.org/index.cfm?pageID=665

Henshel, D. S., Deckard, G., & Buchler, N. (2016). Predicting proficiency in cyber defense team exercises. In *Military Communications Conference, MILCOM 2016-2016 IEEE* (pp. 776-781): IEEE.

Hogan, K. M., Olson, G. T., & Angelina, M. (2020). A Comprehensive Analysis of Cyber Data Breaches and Their Resulting Effects on Shareholder Wealth. *Available at SSRN 3589701*, pg. 25. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3589701

Hunsinger, D. S. (2005). *Predicting the Intention of Managers to use IT Certification in the Hiring Process*, Ann Arbor.

Hunsinger, D. S., Smith, M. A., & Winter, S. J. (2010). A framework of the use of certifications by hiring personnel in it hiring decisions. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems, 42*(1), 9-28. doi:10.1145/1952712.1952714

Iasiello, E. (2014). Is cyber deterrence an illusory course of action? *Journal of Strategic Security, 7*(1), 54-67.

Killcrece, G., Kossakowski, K.-P., Ruefle, R., & Zajicek, M. (2003). *State of the Practice of Computer Security Incident Response Teams (CSIRTs) (Report No. CMU/SEI-2003-TR-001)*, Pittsburgh, PA.

Kim, T. K. (2015). T test as a parametric statistic. *Korean journal of anesthesiology, 68*(6), 540.

Knapp, K. J., Maurer, C., & Plachkinova, M. (2017). Maintaining a Cybersecurity Curriculum: Professional Certifications as Valuable Guidance. *Journal of Information Systems Education, 28*, 101-114. Retrieved from http://jise.org/Volume28/n2/JISEv28n2p101.html

Knowles, W., Such, J. M., Gouglidis, A., Misra, G., & Rashid, A. (2017). All That Glitters Is Not Gold: On the Effectiveness of Cybersecurity Qualifications. *Computer, 50*, 60-71. doi:10.1109/MC.2017.4451226

Kshetri, N. (2009). Positive externality, increasing returns, and the rise in cybercrimes. *Communications of the ACM, 52*(12), 141-144.

Lasheen, M. A. (2015). Technical Certifications in Information Technology as Compared to Traditional Academic Credentials: Impact on Earnings and Employability. In *Order No. 10102661*. Ann Arbor: ProQuest. Web. 17 Nov. 2018.: Northcentral University.

Mathison, S. (1988). Why Triangulate? *Educational Researcher, 17*(2), 13. doi:10.2307/1174583

National Initiative For Cybersecurity Careers And Studies. (2020). *Incident Response*. US-CERT Retrieved from https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework/incident-response#

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). NIST Special Publication 800-181 National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. *Gaithersburg, MD: National Institute of Standards and Technology (NIST)*. doi:10.6028/NIST.SP.800-181

NIST. (2014). *Framework for Improving Critical Infrastructure Cybersecurity*. National Institute of Standards and Technology

Oxford English Dictionary. *"null hypothesis, n."*: Oxford University Press.

Pierce, S. R. (2009). *Information technology certifier perspectives on areas affecting certification assessments: A phenomenological study*, Ann Arbor.

Poe, L. R. (2018). *The Development Of Information Assurance And Cybersecurity Competency Lists.* (M.S.). Purdue University, Retrieved from https://docs.lib.purdue.edu/dissertations/AAI10808410/

Presser, S., Couper, M. P., Lessler, J. T., Martin, E., Martin, J., Rothgeb, J. M., & Singer, E. (2004). Methods for Testing and Evaluating Survey Questions. *Public Opinion Quarterly, 68*(1), 109-130. doi:10.1093/poq/nfh008

Pritchard, K. (2017). First-Year Teachers' Perceptions of their Readiness for the Classroom. In J. Putnam, S. Brown, K. Greer, & J. Rogers (Eds.): ProQuest Dissertations Publishing.

Privacy Rights Clearinghouse. (2019). Chronology of data breaches: Security breaches 2005–present. *Privacy Rights Clearinghouse*. Retrieved from https://privacyrights.org/data-breaches

Privitera, G. J. (2018). *Research methods for the behavioral sciences*: Sage Publications.

Quantitative Approaches - Center for Innovation in Research and Teaching. (2019). Research Ready: Quantitative Research Certification Program. Grand Canyon University. Retrieved from https://cirt.gcu.edu/research/developmentresources/research_ready/quantresearch/approaches

Ramilli, M. (2018). CERTs, CSIRTs and SOCs after 10 years from definitions. In.

Reid, J., Desmond A. (2012). *Cyber Sentries: Preparing Defenders to Win in a Contested Domain*. U.S. Army War College. Carlisle Barracks, PA. Retrieved from http://www.dtic.mil/get-tr-doc/pdf?AD=ADA561779

Research and Markets. (2018). In *Global Incident Response Service Market 2018-2023: Increasing Incidences of Security Breaches Is Driving Growth - ResearchAndMarkets.Com*: Business Wire (English).

Ruefle, R. (2007). Defining Computer Security Incident Response Teams. In: Carnegie Mellon Universty, disponibile al link https://www. us-cert. gov/bsi ….

SANS Institute. (2018). *Interactive NICE Framework Mapping.* Retrieved from https://www.sans.org/courses/niceframework/

Sarkar, D. (2015, May 14, 2015). US government gets low cybersecurity marks from own federal employees, (ISC)2 survey says. *FierceGovernmentIT*.

Schneider, F. B. (2003). Least privilege and more [computer security]. *IEEE Security & Privacy, 1*(5), 55-59.

Selznick, L. F., & LaMacchia, C. (2017). Cybersecurity liability: How technically savvy can we expect small business owners to be. *J. Bus. & Tech. L., 13*, 217.

Steinke, J., Bolunmez, B., Fletcher, L., Wang, V., Tomassetti, A. J., Repchick, K. M., . . . Tetrick, L. E. (2015). Improving Cybersecurity Incident Response Team Effectiveness Using Teams-Based Research. *SECP-M, 13*(4), 20-29. doi:10.1109/MSP.2015.71

Subedi, D. (2016). Explanatory Sequential Mixed Method Design as the Third Research Community of Knowledge Claim. *American Journal of Educational Research, 4*(7), 570-577. Retrieved from http://pubs.sciepub.com/education/4/7/10

U.S. Bureau of Labor Statistics, Employment Projections program. (2019). Occupational Outlook Handbook, Information Security Analysts. Retrieved from https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

Van der Kleij, R., Kleinhuis, G., & Young, H. (2017). Computer Security Incident Response Team Effectiveness: A Needs Assessment. *FRONT PSYCHOL, 8*, 2179-2179. doi:10.3389/fpsyg.2017.02179

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security, 38*, 97-102.

Wierschem, D., Zhang, G., & Johnston, C. (2010). Information technology certification value: An initial response from employers. *Journal of International Technology and Information Management, 19*(4), 89.

Wilshusen, G. C. (2014). Information Security: Agencies need to improve cyber incident response practices. *GAO Reports*, 55-56. Retrieved from http://www.gao.gov/assets/670/662901.pdf

Yasinsac, A., Erbacher, R. F., Marks, D. G., Pollitt, M. M., & Sommer, P. M. (2003). Computer forensics education. *IEEE Security and Privacy, 99*, 15-23. doi:10.1109/MSECP.2003.1219052

Zyphur, M. J. (2009). WHEN MINDSETS COLLIDE: SWITCHING ANALYTICAL MINDSETS TO ADVANCE ORGANIZATION SCIENCE. *ACAD MANAGE REV, 34*(4), 677-688. doi:10.5465/amr.2009.44885862

Appendix A

National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, NIST Special Publication 800-181 (Newhouse et al., 2017)

Knowledge

K0001:	Knowledge of computer networking concepts and protocols, and network security methodologies.
K0002:	Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
K0003:	Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
K0004:	Knowledge of cybersecurity and privacy principles.
K0005:	Knowledge of cyber threats and vulnerabilities.
K0006:	Knowledge of specific operational impacts of cybersecurity lapses.
K0021:	Knowledge of data backup and recovery.
K0026:	Knowledge of business continuity and disaster recovery continuity of operations plans.
K0033:	Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists).
K0034:	Knowledge of network services and protocols interactions that provide network communications.
K0041:	Knowledge of incident categories, incident responses, and timelines for responses.
K0042:	Knowledge of incident response and handling methodologies.
K0046:	Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.
K0058:	Knowledge of network traffic analysis methods.
K0062:	Knowledge of packet-level analysis.

K0070:	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).
K0106:	Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.
K0157:	Knowledge of cyber defense and information security policies, procedures, and regulations.
K0161:	Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks).
K0162:	Knowledge of cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored).
K0167:	Knowledge of system administration, network, and operating system hardening techniques.
K0177:	Knowledge of cyber-attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).
K0179:	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).
K0221:	Knowledge of OSI model and underlying network protocols (e.g., TCP/IP).
K0230:	Knowledge of cloud service models and how those models can limit incident response.
K0259:	Knowledge of malware analysis concepts and methodologies.
K0287:	Knowledge of an organization's information classification program and procedures for information compromise.
K0332:	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.
K0565:	Knowledge of the common networking and routing protocols (e.g. TCP/IP), services (e.g., web, mail, DNS), and how they interact to provide network communications.

K0624:	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)

Skills

S0003:	Skill of identifying, capturing, containing, and reporting malware.
S0047:	Skill in preserving evidence integrity according to standard operating procedures or national standards.
S0077:	Skill in securing network communications.
S0078:	Skill in recognizing and categorizing types of vulnerabilities and associated attacks.
S0079:	Skill in protecting a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters).
S0080:	Skill in performing damage assessments.
S0173:	Skill in using security event correlation tools.
S0365:	Skill to design incident response for cloud service models.

Abilities

A0121:	Ability to design incident response for cloud service models.
A0128:	Ability to apply techniques for detecting host and network-based intrusions using intrusion detection technologies.

Tasks

T0041:	Coordinate and provide expert technical support to enterprise-wide cyber defense technicians to resolve cyber defense incidents.
T0047:	Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation.
T0161:	Perform analysis of log files from a variety of sources (e.g., individual host logs, network traffic logs, firewall logs, and intrusion detection system [IDS] logs) to identify possible threats to network security.
T0163:	Perform cyber defense incident triage, to include determining scope, urgency, and potential impact, identifying the specific vulnerability, and making recommendations that enable expeditious remediation.
T0164:	Perform cyber defense trend analysis and reporting.
T0170:	Perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on enterprise systems.
T0175:	Perform real-time cyber defense incident handling (e.g., forensic collections, intrusion correlation and tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams (IRTs).
T0214:	Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts.
T0233:	Track and document cyber defense incidents from initial detection through final resolution.
T0246:	Write and publish cyber defense techniques, guidance, and reports on incident findings to appropriate constituencies.
T0262:	Employ approved defense-in-depth principles and practices (e.g., defense-in-multiple places, layered defenses, security robustness).
T0278:	Collect intrusion artifacts (e.g., source code, malware, Trojans) and use discovered data to enable mitigation of potential cyber defense incidents within the enterprise.
T0279:	Serve as technical expert and liaison to law enforcement personnel and explain incident details as required.
T0312:	Coordinate with intelligence analysts to correlate threat assessment data.
T0395:	Write and publish after action reviews.
T0503:	Monitor external data sources (e.g., cyber defense vendor sites, Computer Emergency Response Teams, Security Focus) to maintain currency of cyber defense threat condition and determine which security issues may have an impact on the enterprise.
T0510:	Coordinate incident response functions.

Capability Indicators

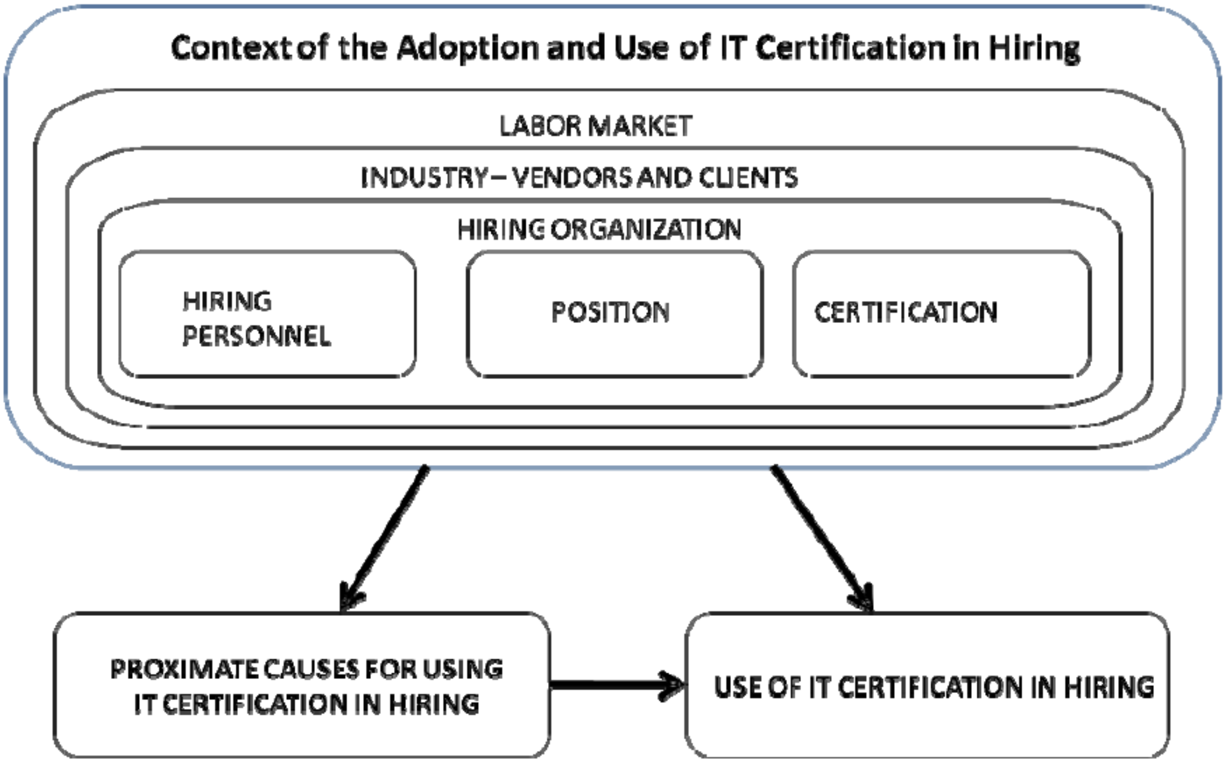
	Entry	*Intermediate*	*Advanced*
Credentials /Certifications	**Recommended**: Yes **Example Types**: N/A **Example Topics**: Certifications addressing new attack vectors (emphasis on cloud computing technology, mobile platforms and tablet computers), new vulnerabilities, existing threats to operating environments, advanced IDS concepts, applications protocols, concepts of TCP/IP and the link layer, DNS, fragmentation, IDS fundamentals and initial deployment (e.g., snort, bro), IDS rules (e.g., snort, bro), IPv6, network architecture and event correlation, network traffic analysis and forensics, packet engineering, silk and other traffic analysis tools, TCP, Tcpdump filters, UDP and ICMP, Wireshark fundamentals	**Recommended**: Yes **Example Types**: N/A **Example Topics**: Certifications addressing incident handling (identification, overview and preparation) buffer overflow, client attacks, covering tacks (networks, systems), denial of service attaches, network attacks, password attacks, reconnaissance, scanning (discovery and mapping, techniques, and defense), session hijacking and cache poisoning, techniques for maintaining access, web applications attacks, worms, bots, and bot-nets	**Recommended**: Yes **Example Topics**: Certifications addressing identification of malicious system and user activity, incident response in an enterprise environment, incident response process and framework, timeline artifact analysis, timeline collection, timeline processing, volatile data collection, filesystem structure and analysis, artifact analysis

	Entry	***Intermediate***	***Advanced***
Continuous	**Recommended**: Yes **Examples**: 40 hours annually (may include participation in annual security conferences)	**Recommended**: Yes **Examples**: 40 hours annually (may include participation in annual security conferences)	**Recommended**: Yes **Examples**: 40 hours annually (may include participation in annual security conferences)
Education	**Recommended**: Yes **Example Types**: Associate's, Bachelor's **Example Topics**: Computer science, cybersecurity, information technology, software engineering, information systems, computer engineering	**Recommended**: Yes **Example Types**: Bachelor's **Example Topics**: Computer science, cybersecurity, information technology, software engineering, information systems, computer engineering	**Recommended**: Yes **Example Types**: Bachelor's, Master's, Ph.D. **Example Topics**: Computer science, cybersecurity, information technology, software engineering, information systems, computer engineering
Experiential Learning	**Recommended**: Yes **Examples**: Malware analysis, digital forensics, data/network analysis, information assurance technician, incident handling	**Recommended**: Yes **Examples**: Malware analysis, digital forensics, data/network analysis, penetration testing, information assurance, leading incident handling	**Recommended**: Yes **Examples**: Malware analysis, digital forensics, data/network analysis, penetration testing, information assurance, trends analysis, quality control analysis, information assurance vulnerability management

	Entry	*Intermediate*	*Advanced*
Training	**Recommended**: Yes **Example Types**: N/A **Example Topics**: System administrator, basic cyber analysis, and operations	**Recommended**: Yes **Example Types**: N/A **Example Topics**: Network security vulnerability, advanced network analysis, basic cyber analysis/operations, network traffic analysis, cyber operator, computer forensics invest and response, information security, information systems, network security, information assurance, troubleshooting, security operations, cryptography	**Recommended**: Yes **Example Types**: N/A **Example Topics**: Intermediate cyber, information security, information systems, network security, information assurance, troubleshooting, security operations, cryptography

Appendix B

Figure 10 Factors influencing the use of IT certification in hiring


Context of the Adoption and Use of IT Certification in Hiring
LABOR MARKET
INDUSTRY – VENDORS AND CLIENTS
HIRING ORGANIZATION
HIRING PERSONNEL
POSITION
CERTIFICATION
PROXIMATE CAUSES FOR USING IT CERTIFICATION IN HIRING
USE OF IT CERTIFICATION IN HIRING

Reprinted from A framework of the use of certifications by hiring personnel in IT hiring decisions. (2010), by Hunsinger, D. S., Smith, M. A., & Winter, S. J.

Appendix C

Survey Instrument

Thank you for participating in this research study titled Efficacy of Incident Response Certification in the Workforce, by Sam Jarocki, a doctoral student at Dakota State University, Beacom College of Computer and Cyber Sciences. This survey will be part of a developing research study towards the examination of Commercial Cyber Security Incident Response (IR)

Related Certifications and hiring practices. The questions are logically based on your answers, which will determine if additional questions are necessary for further clarification or irrelevant based on preceding questions. This survey is voluntary, and there is neither risk nor reward for completion. No analysis or record will be kept for those participants that quit the survey; which you can do at any time by closing the browser window/tab, or by choosing the following answers to the first three questions:

- Question 1: "No"
- Question 2: "Prefer not to respond" OR "No"
- Question 3: "Prefer not to respond OR "No"

Your personnel data will not be distributed. Your answers will be included in statistical analysis and anonymized. Please see SurveyMonkey Privacy Policy for additional information. Personal information, if provided, is used by the researcher only to validate entry and contact respondents for clarification if at all needed. If you choose to provide an email address for subsequent contact, it will be kept secure, and never used in any analysis or reporting of results in this study.

This project has been determined exempt from institutional review board review (Approval #2020A70L-L), and is conducted in accordance with DSU, State of South Dakota, and federal rules and policies This project falls outside of definitions used in federal regulations that govern the protections of human subjects in research under 45 CFR 46.102(e) and (l).

Questions adapted from Appendix B of *A framework of the use of certifications by hiring personnel in it hiring decisions* (2010) by Hunsinger, D. S., Smith, M. A., & Winter, S. J.. ACM SIGMIS Database, 42(1), 9. https://doi.org/10.1145/1952712.1952714 (D. Scott Hunsinger et al., 2010)

Qualifying questions designated by *

1. * Do you agree to the above terms? By selecting "Yes," you consent that you are willing to answer the questions in this survey and are at least 18 years of age?
    - ○ *Yes | No*
2. * What is your job role?
    - ○ *Top-Level Management/ Administrative level*
    - ○ *Departmental / Branch Manager*
    - ○ *Supervisory / Operative Manager*
    - ○ *Technical Lead*
    - ○ *Analyst*
    - ○ *HR / IT Recruiter*
    - ○ *Owner*
    - ○ *Prefer not to respond*
    - ○ *Other (please specify)*

3. * Have you been involved in the observation, hiring, or selection of any person who obtained a Commercial Cyber Security Incident Response (IR) Related Certification?
    - *Yes | No | Prefer not to respond*
4. Are you familiar with any of the following certifications? (NONE is acceptable)
    - *CCE: Certified Computer Examiner*
    - *CEH: Certified Ethical Hacker*
    - *GCFE: GIAC Certified Forensic Examiner*
    - *GCFA: GIAC Certified Forensic Analyst*
    - *GCIH: GIAC Certified Incident Handler*
    - *GCIA: GIAC Certified Intrusion Analyst*
    - *GREM: GIAC Reverse Engineering Malware*
    - *CCFE: Certified Computer Forensics Examiner*
    - *CPT: Certified Penetration Tester*
    - *CREA: Certified Reverse Engineering Analyst*
    - *SCYBER: Cisco Cybersecurity Specialist*
    - *CCNA Cyber Ops*
    - *A+*
    - *Network+*
    - *Security+*
    - *NONE*
    - *Other (please specify incident response (IR) centric certifications only, separate multiple with a semi-colon)*
5. While reviewing job applicants, how often do you check whether the candidate holds an incident response related certification?

- *Never | Rarely | Sometimes | Quite Often | Very Often*

6. Do you prefer hiring people that have obtained an incident response related certification?
   - *No Preference | Slightly Prefer | Prefer | Strongly Prefer | Very Strongly Prefer*
7. Does IR certification assist in any of the following during the hiring process?

   Definitely Not | Probably Not | Neutral | Probably Yes | Definitely Yes

   - *Simplifies the vetting of IR candidates*
   - *Verifies candidate's knowledge base of IR*
   - *Verifies candidate can perform IR job function*
   - *Provides credence/justification on IR candidate choice*
   - *Verifies candidate has expended effort to study and learn IR concepts.*
   - *As a tiebreaker, if the candidate pool is otherwise mostly equal*
   - *Other (Please specify)*
8. Are certifications not specifically in the IR domain (e.g., networking, programming, system administration, etc.) useful in increasing an incident response certification effectiveness?
   - *Useless | Probably Useless | Neutral | Probably Useful | Useful*
9. Does the method an incident response certification test is given, such as in-person, online, and/or proctored vs. non-proctored, make a difference when forming an opinion about the value of the certification?
   - *Definitely Not | Probably Not | Neutral | Probably Yes | Definitely Yes*
10. Is a practical component (e.g., live lab) of an incident response certification process important?

- *Unimportant | Somewhat Unimportant | Neutral | Somewhat Important | Important*

11. How do you feel about vendor-specific vs. vendor-neutral certifications?
    - *Unimportant | Somewhat Unimportant | Neutral | Somewhat Important | Important*
12. Does the influence of marketing (e.g., brand recognition, history of certification) have any bearing on the incident response certification value?
    - *Definitely Not | Probably Not | Neutral | Probably Yes | Definitely Yes*
13. Does the job market in a region influence the value of incident response certifications?
    - *Definitely Not | Probably Not | Neutral | Probably Yes | Definitely Yes*
14. Are some incident response certifications more difficult than others?
    - *Yes | No*
15. For the following certifications, please rank the difficulty:

    UNKNOWN | Novice | Intermediate | Advanced

    - *CCE: Certified Computer Examiner*
    - *CEH: Certified Ethical Hacker*
    - *GCFE: GIAC Certified Forensic Examiner*
    - *GCFA: GIAC Certified Forensic Analyst*
    - *GCIH: GIAC Certified Incident Handler*
    - *GCIA: GIAC Certified Intrusion Analyst*
    - *GREM: GIAC Reverse Engineering Malware*
    - *CCFE: Certified Computer Forensics Examiner*
    - *CPT: Certified Penetration Tester*

- *CREA: Certified Reverse Engineering Analyst*
- *SCYBER: Cisco Cybersecurity Specialist*
- *CCNA Cyber Ops*
- *A+*
- *Network+*
- *Security+*
- *Other (please specify)*

16. Which benefits of an incident response certified job candidate are likely:

Unlikely | Somewhat Unlikely | Neutral | Somewhat Likely | Likely

- *Immediate contribution to IR effort*
- *Ability to train others*
- *Ability to replace others*
- *Ability to lead*
- *Update/Modify/Improve IR process*
- *Respond to an incident that has already occurred*
- *Community participation that provides ongoing support and knowledge sharing*
- *Ability to communicate effectively with a common [IR] vernacular*
- *Other (please specify)*

17. Will, a person who already has several years of IR experience benefit from an incident response certification?
    - *Definitely Not | Probably Not | Neutral | Probably Yes | Definitely Yes*
18. Do you feel the organization receives value from incident response certifications employees complete after being hired?

- *Definitely Not | Probably Not | Neutral | Probably Yes | Definitely Yes*

19. How likely is it that you would recommend one or more incident response certifications to a candidate/employee?
    - *Unlikely | Somewhat Unlikely | Neutral | Somewhat Likely | Likely*
20. If other skills (besides incident response), as part of a broader cyber landscape, are necessary to be an effective incident responder, can IR certifications assist in this regard?
    - *Skills outside of incident response are not necessary to be an effective incident responder.*
    - *Skills outside of incident response are necessary to be an effective incident responder, and IR certifications do not help in this regard.*
    - *Skills outside of incident response are necessary to be an effective incident responder, and IR certifications do help in this regard.*
    - *Please elaborate if possible:*
21. If creating and modifying standard operating procedures are necessary for an incident responder to be effective (e.g., developing and editing analytical IR processes), can certifications help in this regard?
    - *Standard operating procedure creation is not necessary to be an effective incident responder.*
    - *Standard operating procedure creation is necessary to be an effective incident responder, but certifications do not help.*
    - *Standard operating procedure creation is necessary to be an effective incident responder, and certifications do help in this regard.*
    - *Please elaborate if possible:*

22. If an analytical mindset is needed to be an effective incident responder, can IR certifications help in this regard?
    - *An analytical mindset is not necessary to be an effective incident responder.*
    - *An analytical mindset is necessary to be an effective incident responder, but certifications cannot help in this regard.*
    - *An analytical mindset is necessary to be an effective incident responder, and certifications can help in this regard.*
    - *Please elaborate if possible:*
23. Are new incident responders in your organization given the same amount of training regardless of earning a certification?
    - *Yes, all incident responders are given the same training regardless of any IR certifications they may hold.*
    - *No, incident responders with IR certifications are given less training.*
    - *Please elaborate if possible:*
24. If you use IR stages/elements/tiers in your organization, do IR certifications help in progressing to higher levels?
    - *IR Tier levels are not leveraged in my organization.*
    - *IR Tier levels are leveraged in my organization, but IR certifications but do not help in this regard.*
    - *IR Tier levels are leveraged in my organization and IR certifications can help in this regard.*
    - *Please elaborate if possible:*

25. What are the stages/elements/tiers of incident response for an IR analyst in your organization (e.g. Tier 1/2/3, initial alert types, email inbox, shoulder-surfing, on-the-job training, etc.)?
    - *What are the stages/elements/tiers of incident response for an IR analyst in your organization, if any (e.g., Tier 1/2/3, initial alert triage, email inbox, shoulder-surfing, on-the-job training, etc.)?*
26. What skills, knowledge, and abilities (KSA's) do you believe an effective incident responder should possess?

Appendix D

TABLE 26 FAMILIARITY WITH SPECIFIC CERTIFICATIONS (SQN-2) DATA

Familiar with Certifications	*n*	*%*
CCE: Certified Computer Examiner	23	28%
CEH: Certified Ethical Hacker	72	88%
GCFE: GIAC Certified Forensic Examiner	50	61%
GCFA: GIAC Certified Forensic Analyst	49	60%
GCIH: GIAC Certified Forensic Handler	59	72%
GCIA: GIAC Certified Intrusion Analyst	49	60%
GREM: GIAC Reverse Engineering Malware	42	51%
CCFE: Certified Computer Forensic Examiner	25	30%
CPT: Certified Penetration Tester	32	39%
CREA: Certified Reverse Engineering Analyst	7	9%
SCYBER: Cisco Cybersecurity Specialist	19	23%
CCNA Cyber Ops	43	52%
A+	61	74%
Network+	68	83%
Security +	72	88%

TABLE 27 PREFER HIRING CANDIDATES WITH CERTIFICATION (PQN-1) DATA

Preference for Candidates with Certification	*n*	*%*
No preference	18	25%
Slightly prefer	14	19%
Prefer	18	25%
Strongly prefer	16	22%
Very strongly prefer	7	9%
Total	73	100%

TABLE 28 IMPORTANCE OF A PRACTICAL COMPONENT (SQN-7) DATA

Importance of Practical Component	*n*	*%*
Unimportant	2	3%
Neutral	7	10%
Somewhat important	25	34%
Important	39	53%
Total	73	100%

TABLE 29 BENEFITS OF HIRING IR CERTIFIED JOB CANDIDATE (PQN-2) DATA

Benefits of Hiring IR Certified Candidate	*Unlikely*	*Somewhat Unlikely*	*Neutral*	*Somewhat Likely*	*Likely*
	n (%)	n (%)	n (%)	n (%)	n (%)
Immediate contribution to IR effort	1(1%)	5 (8%)	13 (21%)	37 (59%)	7 (11%)
Ability to train others	5 (8%)	6 (9%)	25 (40%)	20 (32%)	7 (11%)
Ability to replace others	2 (3%)	8 (13%)	28 (44%)	22 (35%)	3 (5%)
Ability to lead	8 (13%)	8 (13%)	29 (46%)	12 (19%)	6 (9%)
Can update /improve IR process	2 (3%)	6 (9%)	18 (29%)	29 (46%)	8 (13%)
Can respond to incident that occurs	1 (2%)	3 (5%)	19 (30%)	31 (49%)	9 (14%)
Community participation	2 (3%)	5 (8%)	16 (25%)	27 (43%)	13 (21%)
Can communicate in IR vernacular	2 (3%)	2 (3%)	4 (6%)	29 (46%)	26 (41%)

Appendix E

SQL-1 Word Frequency

Word	Length	Count	Weighted Percentage (%)	Similar Words
networking	10	7	10.94	network, networking
analysis	8	4	6.25	analysis
on-the-job training	3	3	4.69	OJT
operating	9	3	4.69	operating
programming	11	3	4.69	programming
sysadmin	8	3	4.69	sysadmin
system	6	3	4.69	system, systems
communication	13	2	3.12	communication
data	4	2	3.12	data
defense	7	2	3.12	defense
forensics	9	2	3.12	forensics
learn	5	2	3.12	learn
outside	7	2	3.12	outside
admin	5	1	1.56	admin
analytical	10	1	1.56	analytical
anomaly	7	1	1.56	anomaly
behavioral	10	1	1.56	behavioral
certifications	14	1	1.56	certifications
cloud	5	1	1.56	cloud
code	4	1	1.56	code
detection	9	1	1.56	detection
dns	3	1	1.56	dns
documentation	13	1	1.56	documentation
experience	10	1	1.56	experience
exposure	8	1	1.56	exposure

functions	9	1	1.56	functions
infrastructure	14	1	1.56	infrastructure
malware	7	1	1.56	malware
memorize	8	1	1.56	memorize
methodology	11	1	1.56	methodology
neutral	7	1	1.56	neutral
offensive	9	1	1.56	offensive
personable	10	1	1.56	personable
roles	5	1	1.56	roles
science	7	1	1.56	science
skills	6	1	1.56	skills
software	8	1	1.56	software
tools	5	1	1.56	tools
vendor	6	1	1.56	vendor

PQL-1 Word Frequency

Word	Length	Count	Weighted Percentage (%)	Similar Words
networking	10	23	7.03	network, networking
analysis	8	22	6.73	analysis
communication	13	19	5.50	communication, communications
analytical	10	11	3.36	analytic, analytical
procedure	9	11	3.36	procedure
enthusiasm	10	9	2.75	enthusiasm, enthusiastic
chain	5	7	2.14	chain
critical	8	7	2.14	critical
data	4	7	2.14	data
forensics	9	7	2.14	forensics
operating	9	7	2.14	operating
programming	11	7	2.14	programming
sysadmin	8	7	2.14	sysadmin
systems	7	7	2.14	systems
tools	5	7	2.14	tool, tools
team	4	6	1.83	team
thinking	8	6	1.83	thinking
awareness	9	5	1.53	awareness
custody	7	5	1.53	custody
documentation	13	6	1.53	documentation
malware	7	5	1.53	malware
offensive	9	5	1.53	offensive
attention	9	4	1.22	attention
detail	6	4	1.22	detail
methodology	11	5	1.22	methodology
mindset	7	4	1.22	mindset
security	8	4	1.22	security

technical	9	4	1.22	technical
adaptability	12	3	0.92	adaptability
calm	4	3	0.92	calm
engineering	11	3	0.92	engineering
enterprise	10	3	0.92	enterprise
logs	4	3	0.92	logs
memory	6	3	0.92	memory
reverse	7	3	0.92	reverse
compliance	10	2	0.61	compliance
contribution	12	2	0.61	contribution
cooperation	11	2	0.61	cooperation
creation	8	2	0.61	creation
explain	7	2	0.61	explain
fundamentals	12	2	0.61	fundamentals
investigative	13	2	0.61	investigative
kill	4	2	0.61	kill
logic	5	2	0.61	logic, logical
policy	6	2	0.61	policy
prioritization	14	2	0.61	prioritization
science	7	2	0.61	science
skills	6	2	0.61	skills
trend	5	2	0.61	trend, trends
troubleshooting	15	2	0.61	troubleshooting
accountable	11	1	0.31	accountable
admin	5	1	0.31	admin
adversary	9	1	0.31	adversary
appliances	10	1	0.31	appliances
architectures	13	1	0.31	architectures
automation	10	1	0.31	automation
best	4	1	0.31	best

bias	4	1	0.31	bias
building	8	1	0.31	building
business	8	1	0.31	business
certification	13	1	0.31	certification
cloud	5	1	0.31	cloud
code	4	1	0.31	code
collaboration	13	1	0.31	collaboration
command	7	1	0.31	command
compliance	10	1	0.31	compliance
cryptography	12	1	0.31	cryptography
curiosity	9	1	0.31	curiosity
cyber	5	1	0.31	cyber
detachment	10	1	0.31	detachment
different	9	1	0.31	different
direction	9	1	0.31	direction
discretion	10	1	0.31	discretion
evidence	8	1	0.31	evidence
exploitation	12	1	0.31	exploitation
flexible	8	1	0.31	flexible
follow	6	1	0.31	follow
handling	8	1	0.31	handling
hardware	8	1	0.31	hardware
inquisitive	11	1	0.31	inquisitive
integrity	9	1	0.31	integrity
knowledge	9	1	0.31	knowledge
lab	3	1	0.31	lab
leadership	10	1	0.31	leadership
line	4	1	0.31	line
logistics	9	1	0.31	logistics
motivation	10	1	0.31	motivation

organizational	14	1	0.31	organizational
practices	9	1	0.31	practices
processes	9	1	0.31	processes
reading	7	1	0.31	reading
recognition	11	1	0.31	recognition
research	8	1	0.31	research
resolution	10	1	0.31	resolution
resourcefulness	16	1	0.31	resourcefulness
rule	4	1	0.31	rule
sensitivity	11	1	0.31	sensitivity
share	5	1	0.31	share
situational	11	1	0.31	situational
software	8	1	0.31	software
techniques	10	1	0.31	techniques
thinking	8	1	0.31	thinking
use	3	1	0.31	use
vulnerabilities	15	1	0.31	vulnerabilities

PQL-1 Full Word Coding

Name	References
analysis	22
network analysis	9
malware analysis	5
data analysis	4
memory analysis	3
technical analysis	1
network	11
network analysis	9
network admin	1
network security	1
data	7
data analysis	4
data science	2
data sensitivity	1
critical thinking	6
critical thinking	6
malware analysis	5
malware analysis	5
awareness	5
enterprise awareness	3
business awareness	1
situational awareness	1