All That Glitters Is Not Gold: On the Effectiveness of Cyber Security Qualifications

William Knowles, Jose M. Such, Antonios Gouglidis, Gaurav Misra and Awais Rashid

Abstract— There has been a proliferation of industry-focused cyber security qualifications, which use different techniques to assess the competencies of cyber security professionals and certify them to employers. There is, however, a lingering question about these qualifications: do they effectively assess the competencies of cyber security professionals? 74 cyber security qualifications were analysed to determine how competency assessment is performed in practice, and five distinct techniques were identified together with the frequency of their use within qualifications. These techniques formed the basis of a large-scale survey of the perceptions of 153 industry stakeholders on the effectiveness of individual techniques and their cost-effectiveness as combinations. Despite a perceived low effectiveness of Multiple Choice Examinations, industry qualifications were found to rely on it heavily, often as a sole technique, and few qualifications utilised the cost-effective combinations identified by stakeholders.

Index Terms—Cyber Security, Qualifications, Competency

1 Introduction

MUCH has been made of a reported skills shortage within cyber security [1]. Research strands that seek to address this topic have focused on industry professionalisation [2], competency requirements [3], [4], and the design of training programmes [5], [6], with a particular emphasis on the role of competitive events, such as Capture The Flag (CTF) competitions [7], [8], [9], [10]. One core area that has remained unaddressed, however, is a focus on the approaches to assess competency within cyber security qualifications. We must seek to ensure that those who have undergone cyber security training and development are able to effectively turn theory into practice, and that individuals have achieved an appropriate level of expertise.

This is achieved through competency assessment techniques – techniques which generate evidence to provide assurance of particular qualities about the subject under evaluation. A conspicuous and frequently seen example of such a technique within cyber security qualifications is that of the multiple-choice examination. To effectively assure that levels of required expertise are met (as defined on a per qualification basis), we therefore must understand the effectiveness of different techniques in generating such evidence. Equally, it is of importance to understand the economic factors of competence assessments. There is a cost for both exam providers, and a cost for exam takers (either directly or indirectly through a sponsoring organisation), and the result plays a role in incentivising which qualifications are pursued. Despite this, to the authors' knowledge, no research has examined the effectiveness (i.e., the ability to generate accurate evidence of competency) nor cost-effectiveness (i.e., effectiveness relative to the cost of generating evidence) of competency assessment techniques for cyber security.

This study provides a first step in addressing these topics. Through a systematic review of 74 industry-focused cyber security qualification examinations (i.e., as opposed to those offered by academia), five competency assessment techniques were defined: Paper-Based Examination (Multiple-Choice), Paper-Based Examination (Narrative Form), Oral Examination (Viva Voce), Virtual Lab Examination, and Employment History and Qualification Review. The extent to which these five techniques are represented within the 74 qualifications is then analysed, in order to provide insight into industrywide and skill-specific trends towards competency assessment. This was followed by a large scale survey, which gathered the perceptions of 153 industry stakeholders on the characteristics of the defined techniques. Stakeholder perceptions on the effectiveness of each of the five techniques are explored, including how they differ between "Security Practitioner" and "Information Security Manager" roles, which is followed by an examination of perceptions about cost-effective combinations.

It is through the definition and analysis of the industry usage of such techniques that a trend towards a heavy use and reliance upon multiple choice examinations is made explicit. This technique, however, is shown to be perceived as the least effective, while scarcely used techniques, such as virtual lab examinations, are perceived as being notably more effective. Stakeholder-identified cost-effective combinations are further shown to be rarely used in practice. It is on the basis of these analyses that the key finding is presented: the approaches to competency assessment used by cyber security qualifications are perceived to be neither the most effective nor cost-effective by those working within industry.

William, Antonios, Gaurav and Awais are with Security Lancaster, School of Computing and Communications, Lancaster University, LA1 4WA, UK. Jose M. Such is with Department of Informatics, King's College London, WC2R 2LS. Contact author: Jose M. Such, e-mail: jose.such@kcl.ac.uk

2 Related Work (To go as Sidebar)

Research on the development of specialist cyber security knowledge to overcome the sheer and well-known cyber security skills shortage mainly focused to date on 3 streams: competency frameworks, professionalisation, and cyber security challenges and contests.

Competency frameworks are usually employed as a way to develop workforces in specific fields. In cyber security, a holistic approach towards developing workforces is generally recommended through the integration of development strategies into a plan [6]. Competency frameworks already provide support to software security specialists through software assurance competency models [3]. Such models can provide indications about the background and capability needed by security specialists. Other aspects of competency frameworks include education cycles and ground truth knowledge. The former can be used in cyber security for the evaluation of educational interventions [5], [10], while the latter mostly provides an understanding on how attackers compromise systems [11]. Academic accreditations and professional certifications are an important part of such competency frameworks [12], and several guidelines and educational standards were proposed to facilitate the process of defining the field of cyber security [13].

Professionalisation helps identify the required set of (both general and specific) skills for cyber security professionals and establish different professional occupations/roles with their own skill requirements [4]. However, this has to be undertaken at the right pace and not necessarily at the same time for all occupations [2], and existing standard and certification bodies should be rationalised into a single professional body per discrete occupation [14].

Cyber security challenges and contests operate as a pedagogical tool for improving the skills of professionals in safe environments and prepare them for real scenarios [7]. Such challenges have high value since they help develop a security mindset and operate in a complementary way to existing educational approaches [8], regardless of their nature (e.g., hacking competition or military exercise) [9].

While the research streams described above are of critical importance to the development of the cyber security profession, there is a lack of research on approaches to assess competency within cyber security qualifications, particularly on how effective current practices to assess competency are.

3 Competency Assessment Techniques In Industry Qualifications

Understanding the use and role of competency assessment techniques within existing qualifications formed the first stage of the analysis. A qualitative review of 74 qualifications (see Table I) identified five distinct techniques for assessing an individual's competency. A definition was produced for each of these techniques to establish consistent interpretation and understanding for subsequent analyses. The five competency assessment techniques are:

- Virtual Lab Examination - The use of a virtual lab environment to simulate real-world scenarios for testing a candidate's competence.
- Oral Examination (Viva Voce) - The process of questioning and answering using spoken word to determine a candidate's competence.
- Paper-Based Examination (Narrative Form) - An assessment that uses exam papers where questions must be answered in an essay style (i.e., written as a narrative).
- Paper-Based Examination (Multiple-Choice) - An assessment that uses exam papers where questions have multiple pre-prepared answers, of which the candidate must select one or a subset.
- Employment History and Qualification Review - A review of the work history and experience of an individual. This includes the validation of prerequisite qualifications.

These competency assessment techniques are categorised further here based on whether the assessment material presented to the subject under evaluation can be considered to be characterised by a degree of dynamism during the assessment. Therefore, there are the largely "dynamic" techniques (*Virtual Lab Examination* and *Oral Examination (Viva Voce)*), and the largely "static" techniques (*Multiple Choice Examination*, *Narrative Form Examination* and *Employment History and Qualification Review*).

Such definitions provide a foundation for analysing each industry qualification's approach to the competence assessment of cyber security professionals. Table 1 presents the findings of such an analysis and outlines competency assessment techniques used across the 74 qualifications. Here Xrepresents a scenario where the use of a technique is mandatory, while X* indicates its use is optional (e.g., it is case-specific depending upon the body that is performing an assessment).

Multiple Choice Examination Dominates

The frequency with which each competency assessment technique is used across all qualification schemes is illustrated in Figure 1a; these frequencies only represent situations where the technique used is mandatory, as opposed to where it is optional. A clear dominance can be seen for the use of *Multiple Choice Examination*, which features in 60 of the 74 qualifications. Such dominance is potentially a consequence of the ease with which examination material can be produced, and therefore, kept up-to-date. Furthermore, *Multiple Choice Examination* arguably provides the flexibility to assess a broad range of skill-sets, while avoiding an inherent bias towards particular

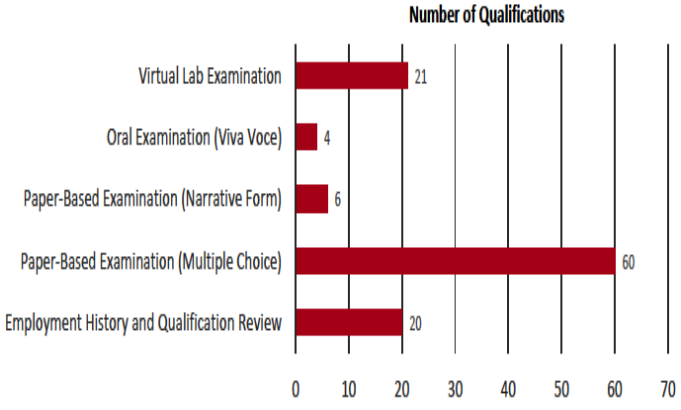
technologies for qualifications that target general security practitioners (e.g., security managers). However, despite this, it is notable that *Multiple Choice Examination* is still frequently used within qualifications for niche skillsets. The second and third ranked competency assessment techniques received similar frequency counts to each other. The second most popular was *Virtual Lab Examination* with 21. It should be noted, however, that this category encompasses multiple implementation strategies which were identified in the analysis, from the single task-oriented, multi-minute duration assessments of qualifications such as CompTIA's Security + to the 24, 48 and 72 hour intensive exams of Offensive Security. *Employment History and Qualification Review* was represented 20 times, which again saw different use cases: namely, qualifications that verify either that a mandatory minimum number of years of industry experience has been obtained, or a pre-requisite qualification has been achieved. In each case, one could argue that this is a non-rigorous implementation of of this competency assessment technique, and does not constitute a detailed analysis.

TABLE 1
COMPETENCY ASSESSMENT TECHNIQUES USED WITHIN QUALIFICATIONS (AS OF *MARCH 2015*)

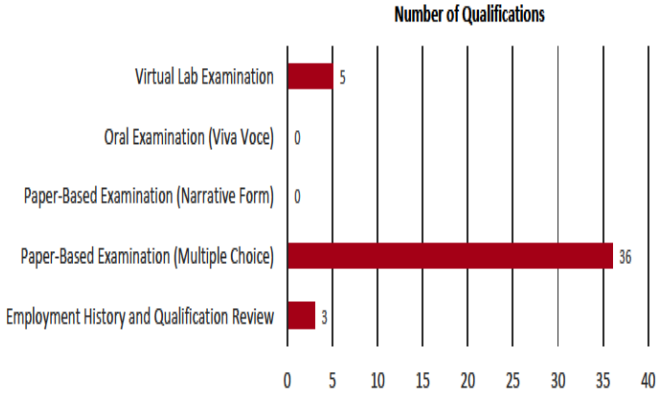
Qualification Body	Qualification Name	Virtual Lab Examination	Oral Examination (Viva Voce)	Paper-Based Examination (Narrative Form)	Paper-Based Examination (MultipleChoice)	Employment History and Qualification Review
CESG	CHECK Team Member	–	–	–	–	✓
	CHECK Team Leader	–	–	–	–	✓
	Certified Professional (CCP)	–	✓*	✓*	✓*	✓
	Listed Advisor Scheme (CLAS)	–	–	–	–	✓
Cisco	Certified Network Associate Security (CCNA Security)	✓	–	–	✓	✓
	Certified Network Professional Security (CCNP Security)	✓	–	–	✓	✓
	Certified Internetwork Expert Security (CCIE Security)	✓	–	–	✓	–
CompTIA	Security+	✓	–	–	✓	–
	Advanced Security Practitioner (CASP)	–	–	–	✓	–
CREST	Practitioner (CPSA)	✓	–	–	✓	–
	Registered Tester (CRT)	✓	–	–	✓	–
	Certified Tester (CCT)	✓	–	✓	✓	–
	Certified Simulated Attack Manager (CCSAM)	✓	–	✓	✓	–
	Certified Simulated Attack Specialist (CCSAS)	✓	–	✓	✓	✓
Cyber Scheme	Associate (CSA)	–	–	–	✓	–
	Team Member (CSTM)	✓	✓	✓	✓	–
	Team Leader (CSTL)	✓	✓	–	–	–
EC-Council	Certified Ethical Hacker (CEH)	–	–	–	✓	–
	Certified Hacking Forensic Investigator (CHFI)	–	–	–	✓	–
	Certified Security Analyst (ECSA)	✓	–	–	✓	–
	Licensed Penetration Tester (LPT)	✓	–	–	–	✓
	Certified Secure Programmer (ECSP)	–	–	–	✓	–
	Network Security Administrator (ENSA)	–	–	–	✓	–
	Certified Chief Information Security Officer (C|CISO)	–	–	–	✓	✓
ISA/IEC 62443	Cybersecurity Fundamentals Specialist	–	–	–	✓	–
ISACA	Certified Information Security Manager (CISM)	–	–	–	✓	✓
	Certified Information Systems Auditor (CISA)	–	–	–	✓	✓
(ISC)²	Certified Information Systems Security Professional (CISSP)	–	–	–	✓	✓
	Systems Security Certified Practitioner (SSCP)	–	–	–	✓	✓
	Certified Authorization Professional (CAP)	–	–	–	✓	✓
	Certified Secure Software Lifecycle Professional (CSSLP)	–	–	–	✓	✓
	Certified Cyber Forensics Professional (CCFP)	–	–	–	✓	✓
	HealthCare Information Security and Privacy Practitioner (HCISPP)	–	–	–	✓	✓
	Certified Cloud Security Professional (CCSP)	–	–	–	✓	✓
ISO 27001	Lead Implementer	–	–	–	✓*	✓*
	Internal Auditor	–	–	–	✓*	✓*

	Lead Auditor	–	–	–	✓*	✓*
Offensive Security	Certified Professional (OSCP)	✓	–	–	–	–
	Wireless Professional (OSWP)	✓	–	–	–	–
	Certified Expert (OSCE)	✓	–	–	–	–
	Exploitation Expert (OSEE)	✓	–	–	–	–
	Web Expert (OSWE)	✓	–	–	–	–
PCI Council	Qualified Security Assessor (QSA)	–	–	–	✓	✓
SANS	GIAC Security Essentials (GSEC)	–	–	–	✓	–
	GIAC Certified Incident Handler (GCIH)	–	–	–	✓	–
	GIAC Certified Intrusion Analyst (GCIA)	–	–	–	✓	–
	GIAC Certified Forensic Analyst (GCFA)	–	–	–	✓	–
	GIAC Penetration Tester (GPEN)	–	–	–	✓	–
	GIAC Security Leadership (GSLC)	–	–	–	✓	–
	GIAC Web Application Penetration Tester (GWAPT)	–	–	–	✓	–
	GIAC Certified Forensic Examiner (GCFE)	–	–	–	✓	–
	GIAC Reverse Engineering Malware (GREM)	–	–	–	✓	–
	GIAC Systems and Network Auditor (GSNA)	–	–	–	✓	–
	GIAC Certified Perimeter Protection Analyst (GPPA)	–	–	–	✓	–
	GIAC Certified Windows Security Administrator (GCWN)	–	–	–	✓	–
	GIAC Information Security Fundamentals (GISF)	–	–	–	✓	–
	GIAC Certified Enterprise Defender (GCED)	–	–	–	✓	–
	GIAC Information Security Professional (GISP)	–	–	–	✓	–
	GIAC Assessing and Auditing Wireless Networks (GAWN)	–	–	–	✓	–
	GIAC Certified UNIX Security Administrator (GCUX)	–	–	–	✓	–
	Global Industrial Cyber Security Professional (GICSP)	–	–	–	✓	–
	GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)	–	–	–	✓	–
	GIAC Secure Software Programmer-Java (GSSP-JAVA)	–	–	–	✓	–
	GIAC Mobile Device Security Analyst (GMOB)	–	–	–	✓	–
	GIAC Network Forensic Analyst (GNFA)	–	–	–	✓	–
	GIAC Certified Web Application Defender (GWEB)	–	–	–	✓	–
	GIAC Law of Data Security & Investigations (GLEG)	–	–	–	✓	–
	GIAC Critical Controls Certification (GCCC)	–	–	–	✓	–
	GIAC Secure Software Programmer- .NET (GSSP-.NET)	–	–	–	✓	–
	GIAC Continuous Monitoring Certification (GMON)	–	–	–	✓	–
	GIAC Security Expert (GSE)	✓	–	–	✓	–
Tigerscheme	Associate Security Tester (AST)	–	–	–	✓	–
	Qualified Security Team Member (QSTM)	✓	✓	✓	✓	–
	Senior Security Tester (SST)	✓	✓	✓	✓	✓

(✓) Mandatory; (✓)Optional; (–) Not Used*



(a) Total Frequency of Use



(b) Frequency of Use as Singular Assessment Method

Fig. 1. Competency Assessment Technique Usage Frequency Within Qualifications

TABLE 2
PERCEPTIONS OF THE EFFECTIVENESS OF COMPETENCY ASSESSMENT TECHNIQUES

Competency Assessment Technique	Excellent	Very Good	Good	Fair	Poor	Total
Virtual Lab Examination	16.4%	29.3%	30.2%	19%	5.2%	116
Oral Examination (Viva-Voce)	11.2%	32.8%	36.6%	16.4%	3%	134
Paper Based Examination (Narrative Form)	3%	31.1%	31.9%	27.4%	6.7%	135
Paper Based Examination (Multiple Choice)	0.7%	14.7%	39.2%	30.8%	14.7%	143
Employment History and Qualification Review	9%	36.8%	30.6%	17.4%	6.3%	144

Despite the similar frequency count of second and third place techniques, there is a distinct divergence in the type of qualifications in which they appear. In the case of *Virtual Lab Examination*, 16 of the 21 qualifications were focused specifically on penetration testing, with the remaining five still largely focused on the role of the practitioner. In contrast, for *Employment History and Qualification Review*, there was a split between those for practitioners and those for more managerial and auditing roles. This split also extended to the types of *Employment History and Qualification Review* required – practitioner qualifications tended to require pre-requisite qualifications, while managerial and auditing qualifications required evidence of industry experience. Interestingly the two remaining competency assessment techniques, *Narrative* only appeared six and four times respectively, and in this was for a penetration testing qualification.

Multiple Choice Examination Frequently Used Alone

The frequency with which competency assessment techniques are used as a singular assessment method are shown in Figure 1b. Of the 60 qualifications that used *Multiple Choice Examination* in the total frequency count of Figure 1a, it was the sole competency assessment technique used in 36, which was split across seven different bodies (CompTIA, Cyber Scheme, EC-Council, PCI Security Standards Council, SANS, Tigerscheme). *Virtual Lab Examination* and *Employment History and Qualification Review* were the only other techniques that featured as the singular method of assessing competency within a qualification; both of which were also second and third ranked for total frequency. *Virtual Lab Examination* was the singular competency assessment technique of choice in five qualifications, and *Employment History and Qualification Review* in three qualifications. In both cases, all qualifications were from the same qualification body (Offensive Security and CESG respectively).

Some Techniques Are Used Optionally

Beyond mandatory competency assessment techniques, there were four qualifications where there is an optional or scheme-specific technique requirement. One of these was the CESG Certified Professional (CCP) scheme, a UK qualification that covers multiple domains of cyber security professionalisation. Assessment is primarily evidence-based through *Employment History and Qualification Review*; however, there are three certification bodies that conduct assessments on behalf of CESG, each of which supplement this using a variation of three other competency assessment techniques (*Multiple Choice Examination*, *Narrative Form Examination* and *Oral Examination (Viva Voce)*). The remaining three qualifications are variations of the auditing qualifications for the information security management system standard ISO/IEC 27001. This presents a unique scenario in that no formal assessment is required for achieving the qualification – instead it is based on the attendance of a 5-day training course. In practice, such courses may finish with an examination, which is usually a *Multiple Choice Examination*; however, the main form of enforcement of quality is through national accreditation bodies, who will mandate that assessments on their behalf can only be conducted by individuals who meet particular requirements (e.g., completion of the course from a trusted qualification body and a number of years of industry experience). Seven further qualifications across three bodies had mandatory training requirements; however, these are simple pre-requisites, and there are further explicitly defined competency assessment techniques for their examinations. These qualifications were the five training courses offered by Offensive Security (for penetration testers), the PCI Security Standards Council QSA (for auditors), and the ISA/IEC 62443 Cybersecurity Fundamentals Specialist (for Industrial Control System security). Beyond training, a further pre-requisite in three qualifications was security clearance. Each qualification was UK-based, namely the CESG CHECK Team Member and Team Leader (for penetration testers), along with the CESG's multi-domain qualification CLAS.

4 PERCEPTIONS ABOUT TECHNIQUES

Based upon the knowledge of "what" competency assessment techniques are used to assess competencies within cyber security qualifications, we can seek to answer the questions: are these approaches effective? In the absence of empirical data to base such a study, an emphasis was placed on gathering the perceptions of those who require such competencies to fulfil their day-to-day roles, and who have potentially been through such

examination processes themselves. The following analyses are therefore based upon the perceptions of a largescale security stakeholder survey that received 153 responses. These stakeholders self-defined their primary roles as: 67% “Security Practitioners” (e.g., security architects, penetration testers, etc.); 18% “Information Security Managers”; 9% “Auditors”; 3% “Competence Assessors”; and 3% “Chief Information Security Officers”. Respondents reported extensive expertise, with 19% declaring over 20 years of experience in the security industry, 45% over 15 years, and 81% over 5 years. For a more detailed breakdown of stakeholder composition, including the qualifications held by the stakeholders, see [15].

What constitutes a competency assessment technique has an abundance of potential variations, which is largely influenced by an individual’s experiences and knowledge; therefore, in order to promote consistency of interpretation the aforementioned definitions were provided to stakeholders during the survey.

Stakeholders were asked to rate their perceived effectiveness for each competency assessment technique using a five level scale. The findings are presented in Table II, which includes the total number of stakeholders that provided answers for each technique.

Not all stakeholders answered each question, and it is notable that those with the highest frequency (*Employment History and Qualification Review* and *Multiple Choice Examination*) were also earlier identified within the qualification analysis to be amongst the most widely used. In contrast, *Virtual Lab Examination* received markedly lower responses. This may be a consequence of the currently limited implementation across qualifications, which is mostly isolated to the penetration testing industry. Stakeholders from other roles may therefore lack confidence in answering questions in an authoritative manner.

Multiple Choice Examination is the Least Effective

Despite the popularity of *Multiple Choice Examination* in the qualifications schemes, it received the largest amount of responses at lower levels with a combined 45.5% at “Fair” and “Poor”. *Narrative Form Examination* was further perceived poorly, including a 27.4% “Fair” rating. Moreover, both *Multiple Choice Examination* and *Narrative Form Examination* were the only techniques to receive a combined score of greater than 60% at the lowest three levels (“Good”, “Fair” and “Poor”) with 84.7% and 66% respectively. At the higher end of the scale, both received low “Excellent” effectiveness scores comparative to other techniques; however, at “Very Good” only *Multiple Choice Examination* was notably anomalous. *Virtual Lab Examination* received the highest “Excellent” rating, but interestingly scored only the second highest for joint “Excellent” and “Very Good” ratings with 45.7% Instead, it was *Employment History and Qualification Review* that was best represented here with 45.8%.

To provide a single score of effectiveness to further the analysis a method was defined for aggregating the responses of the stakeholders. The results for this analysis can be seen in Figure 2 as red bars (we explain the other bars later on). In particular, for each assessment

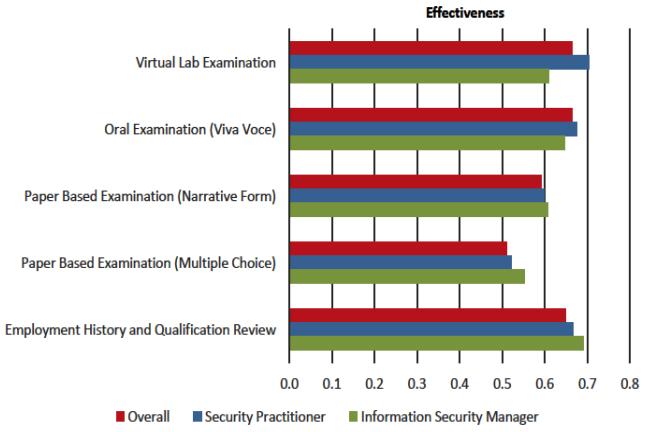


Fig. 2. Effectiveness (see formula in the text) of Competency Assessment Techniques

technique effectiveness was computed as:

Effectiveness =

$$(W_{excellent} \times VP_{excellent} + W_{very\ good} \times VP_{very\ good} + W_{good} \times VP_{good} + W_{fair} \times VP_{fair} + W_{poor} \times VP_{poor})$$

where W were the weightings assigned to levels on the scale as follows:

W = {(Excellent = 1),(Very Good = 0.8), (Good = 0.6),(Fair = 0.4),(Poor = 0.2)}

and VP is the “Valid Proportion” (VP) of stakeholder responses for each level on the scale:

$$VP_{level} = \frac{Level\ Occurences}{Total\ Number\ of\ Levels'}, \text{V P} \in [0,1].$$

VP as defined here consists of the frequency that a particular variable was chosen by survey respondents, relative to the cumulative frequency of all answers, which excludes missing cases (i.e., where respondents did not answer the question). For example, how many respondents answered “Excellent” effectiveness relative to the total number of answers across “Excellent”, “Very Good”, “Good”, “Fair” and “Poor”. VP is then represented within the range of [0,1].

Practitioners Favour “Dynamic” Techniques While Managers Favour “Static” Techniques

In addition to providing an overall score, which represents the holistic view of the security industry from the perspective of our sample, the effectiveness was further assessed specifically for those in the Security Practitioner and Information Security Manager roles (shown as different coloured bars in Figure 2). The remaining roles were not calculated as the sample size was deemed too small to be representative. The two chosen roles do, however, still allow an analysis of perceptions from the perspective of those in practitioner roles versus those in managerial roles.

The single metric for the combined roles tells a familiar story; both *Multiple Choice Examination* and *Narrative Form*

Examination are perceived as the least effective competency assessment techniques. The most commonly used competency assessment technique used within qualifications schemes (*Multiple Choice Examination*) is therefore also perceived to be the least effective, and in many cases, it is often the only competency assessment technique used to assess competency. *Virtual Lab Examination* received the joint highest effectiveness score, as would have been expected from the tabular analysis; however, its companion was *Oral Examination (Viva Voce)* rather than *Employment History and Qualification Review*. The latter did, however, follow closely in third place.

A greater level of insight can be found when examining the subtle changes in ranking that can be seen between stakeholder roles for the two types of competency assessment techniques: "dynamic" (*Virtual Lab Examination* and *Oral Examination (Viva Voce)*) and "static" (*Multiple Choice Examination*, *Narrative Form Examination* and *Employment History and Qualification Review*). Information Security Managers tend to favour the static, while Security Practitioners favour the dynamic. In the case of all static techniques it is notable that both Information Security Managers and Security Practitioners perceived a higher effectiveness than the overall role, which suggests this latter score was influenced negatively by the omitted roles. The greater perceptions of effectiveness here, however, were from Information Security Managers. In contrast, for dynamic techniques, Security Practitioners reported higher effectiveness scores than the overall role, while Information Security Managers perceived an effectiveness score that was lower than the overall role. In particular views are markedly divergent for *Virtual Lab Examination*. However, a Mann-Whitney U Test did not find the difference between Information Security Managers and Security Practitioners to be statistically significant for any of the assessment techniques, so this should be further analysed in the future.

Which are the most Cost-Effective Combinations of Techniques?

As highlighted within the analysis of qualifications, competency assessment techniques are frequently not used to assess competency in isolation, but instead are often combined, which can have a synergistic effect on effectiveness. This synergy, however, comes with an associated additional cost, which must be balanced in relation to the effectiveness. To identify costeffective combinations of competency assessment techniques, stakeholders were asked to select which combination they deemed to be the most cost-effective. The results of this analysis can be seen in Figure 3. The particular question gave practitioners the option to select all the assessment techniques (from the five considered) they thought would constitute the most cost-effective combination. The items represented within this figure are the frequency that each combination was selected by stakeholders. Role-specific frequencies are also included; however, any interpretation of these values should consider the disparity in the number of Information Security Managers and Security Practitioners that took part in the study.

The most cost-effective combination by a notable margin was Comb. 3 (*Oral Examination (Viva Voce)* and *Employment History and Qualification Review*), whose constituent competency assessment techniques also rated highly for effectiveness. That was not the case for the second ranked Comb. 8 (*Multiple Choice Examination* and *Employment History and Qualification Review*), however, which contained competency assessment techniques at both ends of the effectiveness spectrum. Comb. 8 was closely followed by the jointly ranked Comb. 1 (*Virtual Lab Examination* and *Oral Examination (Viva Voce)*) and Comb. 9 (*Oral Examination (Viva Voce)*, *Narrative Form Examination* and *Employment History and Qualification Review*). Although caution must be taken in a role-based analysis it is notable that for the top-ranked Comb. 3 there is a higher proportion of Information Security Managers than would be otherwise expected, while the opposite is true for Comb. 8 and Comb. 1. Within these combinations there is no clear dominance of either competency assessment technique type. The highest frequency combinations with the exception of Comb. 1, consist of both static and dynamic competency assessment techniques – in particular *Employment History and Qualification Review* and *Oral Examination (Viva Voce)* respectively.

Multiple combinations received few votes. Caution should be taken in labelling these the least cost effective combinations due to the nature of the question proposed to stakeholders; more appropriately, they can be considered the *least, most cost-effective*. That said, however, there are only 26 combination possibilities, and 24 are represented. The two missing combinations are: Comb. 25 (*Multiple Choice Examination* and *Narrative Form Examination*); Comb. 26 (*Virtual Lab Examination*, *Multiple Choice Examination* and *Narrative Form Examination*). These combinations were omitted from Figure 3 due to not being selected by stakeholders. Of the six lowest ranked combinations, *Multiple Choice Examination* and *Oral Examination (Viva Voce)* both appear five times, with every one of the six combinations having one or more of the paper-based examinations.

Which techniques appear most frequently in Cost-Effective Combinations?

One metric that is not explicitly apparent in Figure 3 is the total frequency that each individual competency assessment technique appears across all combinations. By a considerable margin the two most frequent were *Employment History and Qualification Review* and *Oral Examination (Viva Voce)* with 96 and 81 votes respectively. Although *Virtual Lab Examination* had the fewest responses in the effectiveness analysis, it was also well represented here with 69 votes. In contrast, *Narrative Form Examination* received only 51, while *Multiple Choice Examination* received less than half of the most frequent technique with 47. The two least effective competency assessment techniques were therefore also the least frequently selected within cost-effective combinations. Despite this they are still well represented in the most costeffective combinations – four of the top six combinations have at least one paper-based

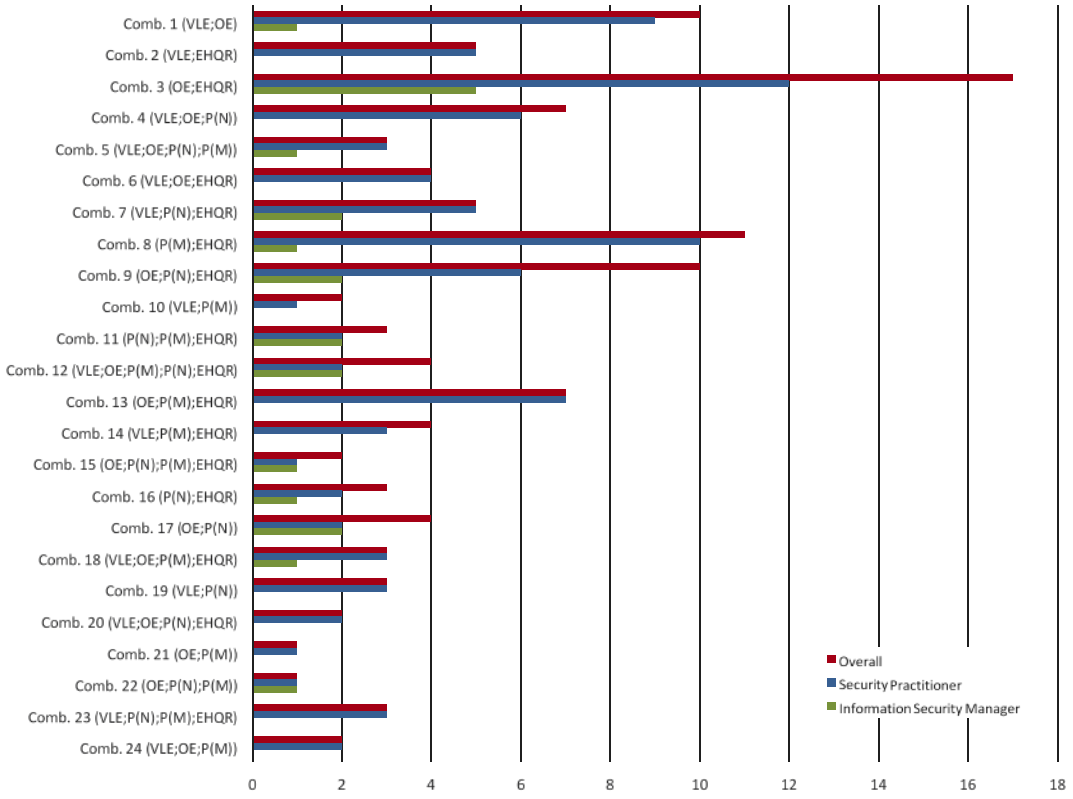


Fig. 3. Cost-Effectiveness of Competency Assessment Technique Combinations – (VLE) Virtual Lab Examination; (OE) Oral Examination (Viva Voce); (P(N)) Paper-Based Examination (Narrative Form); (P(M)) Paper-Based Examination (MultipleChoice); (EHQR) Employment History and Qualification Review

examination. This finding is particularly notable for *Multiple Choice Examination* where one argument for its use is the low cost to maintaining up-todate and relevant examination material. The findings suggest, however, once this cost is balanced against the effectiveness provided, other assessment techniques provide a higher perceived value.

Qualifications Rarely Use Cost-Effective Combinations

Across the 74 qualifications that were reviewed, 44 used only a single technique for competency assessment. This figure was reached by excluding qualifications that include optional techniques (i.e., they are considered combinat combinations); therefore, the number that use a single technique may be slightly higher depending upon a particular qualification's implementation. The remaining 30 qualifications were largely dominated by two combinations. Comb. 8 (*Multiple Choice Examination* and *Employment History and Qualification Review*) was the most frequent with 13 qualifications using this approach; this combination was also the second highest rated for cost-effectiveness by stakeholders. Comb. 10 (*Virtual Lab Examination* and *Multiple Choice Examination*) was also used by six qualifications. Unlike Comb. 8, however, Comb. 10 was one of the lowest ranking cost-effective combinations. Three further combinations appeared twice, including Comb. 25 (*Multiple Choice Examination* and *Narrative Form Examination*) which received no votes in the cost-effectiveness analysis. Five combinations appeared only once, including Comb. 12 which is comprised of all competency assessment techniques. Comb. 3 which was perceived to be the most cost-effective combination is not utilised by any qualification. It must be noted, however, that not all qualifications that use multiple competency assessment techniques will perceive cost-effectiveness as the primary desirable metric, which is instead focused heavily on effectiveness (e.g., those that are a prerequisite for doing cyber security work for governments or critical infrastructure sectors, such as some of the UK penetration testing qualifications).

5 CONCLUSION

This study sought to answer questions surrounding the current and potential future approaches to assessing the competencies of cyber security professionals. A review of competency assessment technique use within 74 qualifications was performed. These results were then contextualised through an analysis of the perceptions of 153 industry stakeholders on the effectiveness of individual techniques and the costeffectiveness of combinations.

The findings identified that the least effective competency assessment technique was *Multiple Choice Examination*; however, it was also a technique found to have mandatory use in 60 of 74 (81%) of qualifications, while also

being the singular technique used in 35 qualifications (47%). Therefore, a large proportion of current cyber security industry qualifications are using an approach that is perceived to be the least effective. In contrast, *Oral Examination (Viva Voce)*, *Virtual Lab Examination* and *Employment History and Qualification Review* were perceived to be notably more effective. The latter two were the second and third most frequently used mandatory techniques within qualifications, but far less frequent, being found in 21 (28%) and 19 (26%) qualifications respectively. A slight bifurcation in technique preference was further identified between those of the Security Practitioners and Information Security Manager roles, with former favouring dynamic techniques, and the latter the static.

Out of the 74 qualifications, 30 (41%) were identified to use two or more competency assessment techniques. The most common combination used in practice (13 out of 74 qualifications) was Comb. 8 (*Multiple Choice Examination* and *Employment History and Qualification Review*), which stakeholders perceived to be the second most cost-effective combination. The most cost-effective, Comb. 3 (*Oral Examination (Viva Voce)* and *Employment History and Qualification Review* was not used by any qualifications.

The main limitation of the findings presented here center around the use of perception which is a subjective measure, and therefore must be interpreted with caution. To some extent perception acts as an advantage when the focus is on understanding competencies. This is most evident with the analysis of effectiveness – an individual will be ideally suited to judge which techniques best assess the competency required to fulfil their day-to-day specialism. However, the perceptions of individuals about cost are likely to be influenced by the price that individuals have paid as examination fees. Future research should seek to engage with qualification bodies to gain further insights on the actual cost of designing, invigilating, and marking such examinations.

This paper has presented data that suggests many cyber security qualifications are using approaches to competency assessment that are perceived as neither effective nor costeffective – something that raises concerns as the industry attempts to address the cyber security skills gap. Two areas of future research are proposed by the authors. First, examining which techniques are appropriate for assessing more granular role types (e.g., breaking Security Practitioner into security architect and penetration tester). Second, an assessment of cost-effectiveness that includes a quantitative metric of cost – similar to what has already been done for assurance techniques [16]. Such research would likely need to be facilitated by qualification bodies in order to be representative.

ACKNOWLEDGMENT

This cyber security project was sponsored by the UK Government.

REFERENCES

[1] T. Caldwell, “Plugging the cyber-security skills gap,” *Computer Fraud & Security*, vol. 2013, no. 7, pp. 5–10, 2013.

[2] D. L. Burley, J. Eisenberg, and S. E. Goodman, “Would cybersecurity professionalization help address the cybersecurity crisis?” *Communications of the ACM*, vol. 57, no. 2, pp. 24–27, 2014.

[3] T. B. Hilburn and N. R. Mead, “Building Security In: A Road to Competency,” *IEEE Security & Privacy*, vol. 11, no. 5, pp. 89–92, 2013.

[4] L. E. Potter and G. Vickers, “What Skills do you Need to Work in Cyber Security?” in *Proc. 2015 ACM SIGMIS-CPR*. ACM Press, 2015, pp. 67–72.

[5] M. Dark and J. Mirkovic, “Evaluation Theory and Practice Applied to Cybersecurity Education,” *IEEE Security & Privacy*, vol. 13, no. 2, pp. 75–80, 2015.

[6] L. Hoffman, D. Burley, and C. Toregas, “Holistically Building the Cybersecurity Workforce,” *IEEE Security & Privacy*, vol. 10, no. 2, pp. 33–39, 2012.

[7] G. Conti, T. Babbitt, and J. Nelson, “Hacking Competitions and Their Untapped Potential for Security Education,” *IEEE Security & Privacy*, vol. 9, no. 3, pp. 56–59, 2011.

[8] E. Gavas, N. Memon, and D. Britton, “Winning Cybersecurity One Challenge at a Time,” *IEEE Security & Privacy*, vol. 10, no. 4, pp. 75–79, 2012.

[9] C. Eagle, “Computer Security Competitions: Expanding Educational Outcomes,” *IEEE Security & Privacy*, vol. 11, no. 4, pp. 69–71, 2013.

[10] J. Mirkovic, M. Dark, W. Du, G. Vigna, and T. Denning, “Evaluating Cybersecurity Education Interventions: Three Case Studies,” *IEEE Security & Privacy*, vol. 13, no. 3, pp. 63–69, 2015.

[11] M. J. Assante and D. H. Tobey, “Enhancing the cybersecurity workforce,” *IT Professional Magazine*, vol. 13, no. 1, p. 12, 2011.

[12] M. Bishop and D. Frincke, “Academic degrees and professional certification,” *IEEE Security & Privacy*, vol. 2, no. 6, pp. 56–58, 2004.

[13] S. Cooper, C. Nickell, V. Piotrowski, B. Oldfield, A. Abdallah, M. Bishop, B. Caelli, M. Dark, E. K. Hawthorne, L. Hoffman *et al.*, “An exploration of the current state of information assurance education,” *ACM SIGCSE Bulletin*, vol. 41, no. 4, pp. 109–125, 2010.

[14] R. Reece and B. C. Stahl, “The professionalisation of information security: Perspectives of uk practitioners,” *Computers & Security*, vol. 48, pp. 182–195, 2015.

[15] J. M. Such, A. Gouglidis, W. Knowles, G. Misra, and A. Rashid, “The Economics of Assurance Activities,” Security Lancaster, Lancaster University, Tech. Rep. SCC-2015-03, 2015.

[16] J. M. Such, A. Gouglidis, W. Knowles, G. Misra, and A. Rashid, “Information Assurance Techniques: Perceived cost effectiveness”, Computers & Security, vol. 60, pp. 117-133, 2016.

Dr. William Knowles was awarded a PhD by Lancaster University in 2016, funded by an EPSRC Industrial Case PhD that was supported by the Airbus Group (formerly EADS), where he conducted research around security assessments of Industrial Control System environments. This PhD was undertaken at Security Lancaster, an EPSRC-GCHQ Academic Centre of Excellence in Cyber Security Research. He is also a Tigerscheme Qualified Security Team Member (QSTM) penetration tester and ISO/IEC 27001:2013 Lead Auditor. Contact him at w.knowles@lancaster.ac.uk.

Dr. Jose M. Such is Senior Lecturer (Associate Professor) in Computer Science at King's College London. His research interests are at the intersection between cyber security, artificial intelligence, and human-computer interaction; with a strong focus on privacy, intelligent access control, co-owned data, and security controls and assurance techniques in socio-technical and cyber-physical systems. Previously, he was Lecturer in Cyber Security at Lancaster University from 2012 to 2016, and research associate at Universitat Politecnica de Valencia, by which he was awarded a PhD in Computer Science in 2011. Contact him at jose.such@kcl.ac.uk.

Dr. Antonios Gouglidis is a Senior Research Associate at Lancaster University, and currently involved in the EU FP7 funded project HyRiM. Previously, he has worked in academia as a Security Researcher; in industry as a Software Engineer; and in the public sector as an IT Training Consultant. He received his PhD in Applied Informatics from University of Macedonia, Greece; MSc in Mathematics from the Aristotle University, Greece; MSc in Computer Science from Lancaster University, UK; and BSc in IT Engineering from the Alexander Technological Educational Institute of Thessaloniki, Greece. His research interests include security, resilience, access control, and formal methods. Contact him at a.gouglidis@lancaster.ac.uk.

Gaurav Misra is currently a PhD student at Security Lancaster, an EPSRC-GCHQ Academic Centre of Excellence in Cyber Security Research. His research is geared toward development of more usable and effective privacy preserving techniques and mechanisms in social media networks. More specifically, his work is aimed at improving access control mechanisms for social media users. He received his MSc in Computer Security from University of Twente, The Netherlands; and B.Tech in Information Technology from West Bengal University of Technology, Kolkata, India. Contact him at g.misra@lancaster.ac.uk.

Professor Awais Rashid is Director of Security Lancaster Institute, one of the UK's Academic Centres of Excellence in Cyber Security Research. His research interests focus on security of cyber-physical systems (CPS) and studies of adversarial and non-adversarial behaviours pertaining to cyber security. He leads a number of research projects, including a project as part of the Research Institute in Trustworthy Industrial Control Systems (RITICS). He also co-leads the Security and Safety theme within the UK hub (PETRAS) on Security, Privacy and Trust in the Internet of Things and a major programme of research on developing a Cyber Security Body of Knowledge (CyBOK). Contact him at marash@comp.lancs.ac.uk.