How the Certified Information Systems Security Professional Certification Supports Digital Forensic Processes

S.Rule, A.Stander and J.Ophoff

Department of Information Systems, University of Cape Town
e-mail: Samantha.Rule@uct.ac.za

Abstract

This paper explores whether a relationship exists between the Certified Information Systems Security Professional (CISSP) certification and digital forensics. The key findings show that the CISSP Common Body of Knowledge (CBK) covers a wide spectrum of information security practices, processes, and procedures and that the CISSP certification can provide a basic introduction to digital forensic processes and concepts from an incident response perspective. However, the CISSP certification does not bestow an in depth knowledge of digital forensic processes upon those who attain this certification. The CISSP CBK therefore does not support digital forensic processes beyond providing a basic understanding of what digital forensics is and the general concepts found within the digital forensic realm.

Keywords

Digital Forensics, Certified Information Systems Security Professional

1. Introduction

It is often thought that an individual with Certified Information Systems Security Professional (CISSP) Information Security certification does not need additional specialised skills to handle digital forensic incidents. Very little research exist to show if this viewpoint is correct and with the increase of cybercrime in recent years, it is important to know if organisations are adequately equipped to handle incidents of this nature.

This paper shows how the Certified Information Systems Security Professional (CISSP) Information Security certification supports digital forensic processes, with a particular interest in incident response from both an information security perspective as well as from a digital forensic readiness perspective.

The following sections provide some background on the CISSP certification, as well as the digital forensic concepts under investigation.

2. The CISSP Common Body of Knowledge

According to Tittel and Stewart (2003) the very essence of the CISSP is contained in the Common Body of Knowledge (CBK) which divides the field of information

security into ten distinct domains. The CBK forms the basis for the (ISC)² education and certification programs and is regularly updated to ensure that it stays abreast of the fast pace of changing technologies and the ever growing number of creative ways that alleged criminals find to circumvent security controls (Harris, 2008).

The CISSP focuses on generally accepted concepts, techniques and approaches to designing, implementing and maintaining strong effective information security. Less focus is given to the details involved in creating security policies, practices, and procedures. This means that although the CISSP certification can equip an information security specialist to understand digital forensic concepts and processes, it does not necessarily make the information security specialist a digital forensic expert.

The following subsections review the CBK domains relevant to digital forensic processes.

2.1. Legal regulations, compliance, and investigations

This domain (formally known as law, investigations and ethics) covers general computer crime legislation, regulations and investigative measures and techniques used to determine if an incident has occurred as well as the gathering, analysis and management of evidence if it exists. Tittel and Stewart (2003) assert that individuals wishing to obtain the CISSP credential should ensure that they are familiar with relevant cybercrime laws and regulations as well as the proper investigative techniques to gather evidence and incident handling.

2.2. Telecommunications and network security

In this domain the transmission methods, transport format and security measures used to provide confidentiality, integrity, availability and authentication for transmission over private and public networks and media is discussed. According to Tittel and Stewart (2003) CISSP candidates should understand and be able to perform security reviews of email systems, telephony communications, as well as network attacks and counter measures.

2.3. Information security and risk management

Information security management establishes the foundation for a broad and all-inclusive security program to ensure the protection of an organisation's information assets. Information security management communicates the risks accepted by the organisation due to the currently implemented security controls and continually works to cost effectively enhance the controls to minimise the risk to the organisation. Risk management involves being able to perform data classification and risk assessments which will classify the organisation's assets, identity the threats and rate the vulnerabilities so that the necessary controls can be implemented (Bell, 2010).

2.4. Access control

It is important to be able to identify, authenticate, authorise, and monitor who or what is accessing the assets of the organisation, as this is vital information required to protect the assets from vulnerabilities and threats. According to Tittel and Stewart (2003) CISSP candidates need to understand how to plan, design and implement numerous authentication and access control systems. They also need to be able to monitor and audit the efficiency of the controls implemented.

2.5. Physical security

Physical security incorporates the security from the outside perimeter of a facility to the inside office space, including all information security systems (Bell, 2010). CISSP candidates need to understand and be familiar with the concepts affecting physical security as well as the possible security threats. This includes threat prevention and detection and being able to respond to these alerts or alarms (Tittel and Stewart, 2003).

2.6. Operations security

The security principal of availability is the core goal for operations security. Operations security is used to identify the controls placed on hardware, media, and the people who administer and have privilege access to any of the resources. Monitoring and auditing are the mechanisms used to identify any security events and report the information to the appropriate individual, group of individuals or system (Bell, 2010).

3. Incident Response

It is important for organisations to be prepared for security incidents that could take place due to the sharp rise in cybercrime. According to Tipton and Henry (2007) incident response or incident handling has become a primary function of today's information security professionals. Mandia (2003) describes incident response as a multifaceted discipline as it requires resources from various operational units found within an organisation such as human resources, technical experts, security professionals, business managers, legal advisors and end users. Any of these individuals could find themselves involved with responding to a security incident.

Many organisations establish a team of individuals who have special expertise, referred to as a Computer Security Incident Response Team (CSIRT). The CSIRT steps into action and immediately responds when a security incident occurs. A security incident can be defined as any negative event that takes place, during which some aspect of computer security has been threatened or compromised, where there is a loss of data confidentiality, a disruption of data or system integrity, or a disruption to (or denial of) data or system availability (Grance et al., 2008).

CISSP candidates must be familiar with the following set of procedures for incident response.

3.1. Triage

The term triage refers to the sorting, categorising and prioritising when an incident occurs. Triage encompasses the detection, identification and notification sub-phases. In triage incident handlers need to take in all the information available, investigate its severity and then set priorities on how to deal with the incident.

3.2. Reaction

According to Harris (2008) this includes the following phases of incident response. In the containment phase the damage must be mitigated and once the incident has been contained, an analysis of what took place during the incident must be conducted. Next, in the analysis phase, more data is gathered to understand how the incident took place. Finally, in the tracking phase, the source of the incident is identified, if the incident was internal or external, and how the source of the incident was accessed.

3.3. Follow-up

Once the incident is understood, the next stage is the follow up stage which is where the necessary fix is implemented to prevent this type of incident from occurring again in the future (Harris, 2008).

4. Digital Forensic Readiness

A digital forensic investigation is a process to determine and relate extracted information and digital evidence to produce accurate information for review by a court of law. The digital forensic investigation procedures developed by traditional forensic scientists focused on the procedures in handling evidence, while the procedures developed by the technologists focused on the technical details in capturing evidence. Many digital forensic investigators have chosen to follow the technical procedures and forget about the purpose and core concept of a digital forensic investigation. For this reason, legal practitioners sometimes have difficulty in understanding the processes and tasks involved in digital investigations (Ieong, 2006).

An important concept following on from forensic investigation is digital forensic readiness. This is defined as the ability of an organisation to maximise the use and collection of digital evidence while minimising the costs of a forensic incident investigation (Rowlingson, 2004). Digital forensic readiness equips an organisation with processes and procedures to follow when a digital forensic incident has occurred. The goal of these steps is to ensure that the operations and infrastructure are able to fully support an investigation (Carrier and Spafford, 2003).

According to Rowlingson (2004) a framework for digital forensic readiness should contain the following ten steps:

1. Identify the various business scenarios and processes where there is digital evidence, and reduce the impact of any digital crime.

2. Identify the types of digital evidence and their sources, and to know and understand what evidence is available across all the systems and applications used by the organisation.
3. Produce an evidence requirement statement so that those responsible for managing the business risk can communicate with those running and monitoring the information systems through an agreed requirement for evidence.
4. Ensure that any evidence collected is preserved as an authentic record.
5. Secure evidence for a longer period; off-line storage of data may be required for evidence at a later date. Digital evidence must at all times, be secure and tamper-proof.
6. Understand and document what processes or events must be monitored and audited in order to detect incidents before they take place.
7. Know how and when to react to a formal investigation.
8. Ensure that forensic awareness training is developed and provided for the organisation's employees.
9. Produce a policy that describes how an evidence case should be assembled.
10. Have legal advisors review the case file from a legal standpoint.

The following section will examine the research results of how the CISSP certification supports digital forensic processes.

5. Research Data

The sample group selected for the research comprised members of the Information Security Group Africa and members of the Special Interest Groups for Forensics and eCrime. This particular sample was selected as information security, and in particular digital forensics, is a highly specialised field. All of the respondents were individually contacted about participation in the research. An Likert-style electronic survey questionnaire was sent to 25 respondents, from which 16 completed responses were received.

The 16 respondents hold various professional certifications: 11 respondents currently hold the CISSP credential from (ISC)², while 10 respondents hold certifications that were not listed. Two of the respondents hold digital forensic specific qualifications, the GIAC Certified Forensic Analyst, the Certified Forensic Examiner and the vendor specific certification, the AccessData certified Examiner.

The research was aimed at information security professionals and digital forensic investigators in order to establish whether CISSP certified information security professionals are able to assist digital forensic practitioners. As of 2009 (ISC)² had certified 66,000 individuals globally and it could be of great value to the digital forensic discipline to be able to leverage and make use of these individuals.

The main limitation that was observed was the small number of information security professionals who either work in digital forensics or are CISSP certified. With only 16 responses and the limitation of focusing on a small geographical location (South Africa) the findings may be insignificant as there are a much smaller group of CISSPs and digital forensic investigators located in South Africa versus globally.

Despite these limitations it is believed that the overall research findings are still relevant.

The following subsections analyse the data collected by the research. The analysis is grouped according to the research questions.

5.1. Research question 1: Does the CISSP support digital forensics?

Respondents had to rate how relevant each domain of the CISSP was to digital forensics. The following domains were rated most relevant, in descending order: Legal regulations, compliance and investigations (87.5%); Telecommunications and network security (81%); Access controls (75%).

Legal Regulations compliance and Investigations was rated as either relevant or very relevant by 87.5% (14 out of 16) of respondents. A further 64% of these respondents currently hold the CISSP certification. Comments provided by respondents in support of their answer showed that the reasons for selecting relevant or very relevant included, "The legal/law domain is just as important an area of the forensic environment. The content is however not purposefully supportive of digital forensics; but does interact with various sections as mentioned above".

The domain "telecommunications and network security" was rated either relevant or very relevant by 81% (13 out of 16) of the respondents, a further 70% of these respondents currently hold the CISSP credential. 75% (12 out of 16) of the respondents rated "Access controls" as either relevant or very relevant, a further 75% of these respondents hold the CISSP credential.

The following domains were rated least relevant, in descending order: Business Continuity, compliance and investigations (56%); Security Architecture and design (31%).

Business continuity compliance and investigations was rated as the least relevant to digital forensics by 56% (9 out of 16) of the respondents. 75% of these respondents currently hold the CISSP certification. 31% (5 out of 16) of the respondents rated security architecture and design as having some relevance, for how it relates to digital forensics. All of these respondents are CISSP certified.

Does being CISSP certified enable an individual to be able to conduct a digital forensic investigation? 62% (10 out of 16) of respondents disagreed or disagreed strongly that the CISSP certification enabled an individual to conduct a digital forensic Investigation. 60% of the 10 respondents who either disagreed or strongly disagreed currently hold the CISSP certification. Some comments provided by respondents in support of their answer included: "There is very little forensic information in the CBK"; "CISSP CBK covers a wide range of topics with very little depth"; "With a CISSP being a more theoretical accreditation, it would in my eyes not provide much benefit to digital forensic investigations on all levels".

Does the CISSP CBK give an individual sufficient knowledge on incident response? 50% (8 out of 16) respondents were undecided whether the CISSP CBK

gave an individual sufficient knowledge on incident response. 62.5% of these 8 respondents currently hold the CISSP certification. One of the comments provided by a respondent to explain the reason for being undecided stated that "the mile wide aspect allows an individual to know a little about most aspects but specialists are required to assist and provide the depth of understanding needed to complete a forensic plan." This echoed the sentiments of most of the respondents who were undecided, citing that the CISSP allowed for a general overview rather than for in depth knowledge.

Does the CISSP certification enable individuals to draft information security policies? 50% (8 out of 16) respondents were undecided about whether or not the CISSP certification enabled individuals to draft security policies. 71% of 7 respondents who currently hold the CISSP credential agreed that the CISSP certification enabled individuals to draft information security policies. Comments provided by the respondents in support of their answer showed the following reasons for agreeing; "it's an excellent management level IS security certification and "the CISSP definitely provides one with a good basic understanding of the underlying principles of security fundamentals, processes, risk assessments".

If you hold a CISSP certification, how do you rate the content covered in the CBK for digital forensics? Taking into account that 50% of the respondents currently hold the CISSP certification, 25% of the respondents indicated that it was covered while 75% of the respondents indicated that there was some coverage of digital forensics in the CISSP CBK. Some comments provided by the respondents include: "The material covers that focus too lightly"; "There is very little forensic information in the CBK"; "Although I do not have a CISSP, I am very familiar with the CBK for it, as while it is an excellent management level IS security certification; it does not address Digital Forensics at anything other than a superficial level in the investigation and legal domain".

Reviewing these comments, it is possible to deduce that these respondents believe that the CISSP CBK does not contain enough information about digital forensics for an individual to be able to conduct a digital investigation.

5.2. Research question 2: To what extent does the CISSP support digital forensic readiness?

The following three questions relating to forensic readiness were asked in the electronic questionnaire.

Is incident response and forensic readiness the same? 56% (9 out of 16) respondents disagree that incident response and forensic readiness is the same. A further 78% of the 9 respondents that disagreed currently hold the CISSP certification. One respondent commented that, "I do believe that it (the CISSP) may be useful in devising a response plan for forensic readiness."

Should organisations include forensic readiness in their information security policies? 81% (13 out of 16) of the respondents agreed or agreed strongly that organisations should include forensic readiness in their information security policies.

62% of the 8 respondents who agreed and agreed strongly currently hold the CISSP credential. One of the respondent's comments stated that, "the CISSP holder will have a thorough understanding of security architectures and where evidence might reside within a particular network."

Does having an incident response plan enable an organisation to be forensic ready? 50% (8 out of 16) of the respondents disagreed or disagreed strongly that having an incident response plan enabled an organisation to be forensic ready. 62% of the 8 respondents that disagreed or disagreed strongly currently hold CISSP credentials.

Analysing the responses from the questionnaire, it can be noted that the CISSP does support digital forensic readiness, but not to the full extent that is required for an organisation to be forensic ready.

5.3. Research question 3: Is there a relationship between security incident response, which a CISSP would investigate, and digital forensic readiness?

The following three questions relating to incident response were asked in the electronic questionnaire.

Should the CSIRT be able to conduct a digital forensic investigation? 50% (8 out of 16) of the respondents agreed or agreed strongly that it is important for the CSIRT to be able to conduct a digital forensic investigation and 87.5% of the 8 of the respondents currently hold the CISSP credential. Comments provided by respondents in support of their answers showed that the reasons for agreeing or agreeing strongly included; "CISSP provides the basic knowledge to conduct an investigation but depending on the nature of the incident and the responder's knowledge and qualifications, a certified Forensic Investigator could be required."

Should law enforcement be contacted when a security incident takes place? 44% (7 out of 16) respondents were undecided whether to contact law enforcement when a security incident takes place. 62.5% of these 7 respondents currently hold the CISSP certification. 44% (7 out of 16) respondents agreed and agreed strongly that law enforcement should be contacted when a security incident takes place. 71% of the 7 respondents that agreed and strongly agreed currently hold the CISSP certification.

Should forensic investigations only be conducted by specialists and trained individuals? 94% (15 out of 16) of the respondents agreed or agreed strongly that forensic investigations should only be conducted by specialists and trained individuals. 67% of the 15 respondents that agreed or agreed strongly currently hold the CISSP credential.

Comments provided by respondents in support of their answers included, "having a certification (CISSP) does assist an individual with being able to do an investigation but at the end of the day real experience and other related courses/certifications specific to Digital Forensics are much more important". This echoed the sentiments of most of the respondents who agreed or strongly agreed, mentioning that the

CISSP allowed for a general overview rather than for in depth knowledge of performing forensic investigations.

5.4. Research question 4: Are there information security principles or processes that support digital forensic readiness?

The following three questions relating to the importance of incident response and forensic readiness for an organisation were asked in the electronic questionnaire.

Is it important to conduct user awareness for incident response and forensic readiness? 81% (13 out of 16) of the respondents answered that it was important or extremely important to conduct user awareness training for incident response and forensic readiness. 69% of the 13 respondents believing it is important or extremely important currently hold the CISSP credential.

How do you rate the importance of a Computer Security Incident Response Team for an organisation? 87.5% (14 out of 16) of the respondents believe that it is important or extremely important that an organisation has a CSIRT. 78.5% of the 14 respondents agreeing that it was important or extremely important to an organisation to have a CSIRT currently hold the CISSP certification.

How important is it for an organisation to have an incident response plan? 100% of the respondents answered that it is extremely important or important that an organisation has an incident response plan. 62.5% 10 of the respondents answered that it is extremely important with 90% of the 10 respondents holding a CISSP certification. The remaining 37.5% (6 out of 16) respondents answered that it was important for an organisation to have an incident response plan. 33% of 6 respondents hold a CISSP certification.

Reviewing the analysis of the data and the respondents' comments, it can be deduced that there are information security principals or processes that support digital forensic readiness.

By its very nature, digital forensics is a reactive process as it responds to an event that has already occurred. Information security on the other hand is a proactive process, placing controls and preventative measures in a bid to prevent security incidents from occurring in the first place.

The main research question attempted to determine how the CISSP certification supports digital forensics. It emerged from the literature and the data analysis that the CISSP CBK broadly covers information security at a high level and is more theoretical than practical. The CBK also gives the information security professional a general introduction to digital forensic investigations especially in the areas of evidence collection and the chain of custody. However, the CISSP CBK does not equip an information security professional with the skills required to be able to perform a digital forensic investigation that will stand up to legal scrutiny. The following quote from one of the respondents succinctly states the current situation: "It will help, but is not necessarily enough knowledge".

6. References

Bell, L., (2010), CISSP Fast Track Certified Information Systems Security Professional, http://www.alctraining.com.au/pdf/cip.pdf (Accessed 22 September 2010)

Carrier, B. and Spafford, E. (2003), Getting physical with the digital investigation process, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.76.757&rep=rep1&type=pdf (Accessed 28 August 2010)

Grance, T., Kent, K. and Kim, B., (2008), Computer security incident handling guide. Retrieved August 24, 2010 from http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

Hancock, B. (2000), Truly certified: Security certifications update, *Computers & Security*, 19(6), pp. 479-480

Harris,S. (2008), *CISSP All-In-One Exam Guide (4e)*, McGraw-Hill, New York

Ieong, R. (2006), FORZA – Digital Forensics investigation framework that incorporate legal issues, *Digital Investigation*, 3(1), pp. 29-36.

Mandia, K., Prosise, C. and Pepe, M. (2003), *Incident response and computer forensics (2e)*, McGraw-Hill/Osborne, California

Rowlingson, R. (2004), A Ten Step Process for Forensic Readiness, *International Journal of Digital Evidence*, 2, pp. 1-28

Tipton, H.F., Henry, K. (2007). *Official (ISC)² Guide to the CISSP CBK* Boca Raton, Florida: Auerbach Publications

Tittel, E., & Stewart, J. M. (2003). Dissecting the CISSP exam. *Certification Magazine*, 5(2), SG11-SG13.