Chapter 5
The Role of Cybersecurity Certifications

Adrian Davis
ObjectTech Group, UK

ABSTRACT

The chapter looks at the burgeoning field of certification for individuals in the field of information security or cybersecurity. Individual information security certifications cover a wide range of topics from the deeply technical to the managerial. These certifications are used as a visible indication of an individual's status and knowledge, used to define experience and status, used in job descriptions and screening, and may define expectations placed on the individual. This chapter examines how these certifications are produced, the subjects they cover, and how they integrate and the various audiences to which the certifications are aimed. The role, the perceived and real value, and benefits of certification within the field of information security both from an individual and an organizational perspective are discussed. Finally, some conclusions on certification are presented.

INTRODUCTION

Information security[1] certifications now form a significant part of the wider information security industry, with a powerful influence on individuals and organizations within that industry. Certifications are often a prerequisite for senior jobs, working in government or for employment in specific roles; they are also widespread across the industry. The major certification bodies – (ISC)^2, ISACA, EC Council and SANS – claim to have trained or have as members well over 500,000 individuals in total. Certification is also a big business, with annual reports from two of the major players in the field ((ISC)^2, 2017 and ISACA, 2017a) both indicating revenue for each of over US$50 million from education, examinations, membership and publications.

DOI: 10.4018/978-1-6684-3554-0.ch005

Before embarking on a review of these certifications, the definition of certification as used in this chapter should be provided. This chapter uses the term certification with the following meaning: "the act of certifying or state of being certified" (Collins, 2018) here we use the last part of the definition to indicate that an individual is in the state of being certified, i.e. they hold a certificate, which is an official document received when a course of study or training is completed.

The chapter is structured as follows. A very brief background is given to explain the rise of information security certifications. This is followed by a review of certification bodies and their characteristics, then an in-depth review of information security certifications at the time of publication. The discussion continues by examining the role of certifications from a personal and organizational perspective, the perceived value and benefit and then the misuse and abuse to which certifications can be put. Finally, some future trends in the field of information security certification are highlighted.

A BRIEF HISTORY OF INFORMATION SECURITY CERTIFICATIONS

Information security – originally computer security – came from an IT background. It was considered to be an IT specialism for a number of years and so didn't really require much in the way of oversight, a single unified voice, certification or qualifications. Typically, certifications were created by one or more groups of willing, interested and altruistic individuals either responding to a perceived need or trying to set a standard that could be readily understood. By setting standards, these groups hoped to both define what made an individual competent and knowledgeable in the field of information security and provide a mechanism to identify those who were perhaps less than capable. There was not the need to submit to scrutiny or oversight as the numbers involved were small, the individuals knew each other and the roles many of the individuals worked in required some form of government vetting and clearance – and most, if not all of the groups were based in the United States. From these beginnings rose the information security certification industry we see today.

Today, there is no one "global body" that can truly claim to represent information security and the individuals in the field. Whilst there are a number of organizations who have global membership and reach, they do not capture everyone who works in the field, nor does everyone in the field want to hold the certifications they offer. Thanks to its multi-disciplinary nature, information/cyber security is a "big tent" and covers more than just technical roles. Thirty-five roles (CyberSN, 2018) related to security have been identified, ranging from the highly technical security analyst to CEO. These example roles – and all 35 – will have widely differing requirements for skills, knowledge and experience; yet all will require some knowledge of information/cyber security. However, for many non-technical roles, possession of certain certifications will not be possible, as they will not possess the relevant skills and experience – and they might never gain them. Examples of these individuals could include those people working in marketing, PR and finance for information security organizations.

From an academic perspective, information security is a new discipline that has been recognized as such for about thirty years or so. It is multi-disciplinary in nature, covering both technical and non-technical subjects, including programming, hardware design and function, networking, economics, law and business as well as security-related topics such as cryptography and risk management. As a result, it has been difficult to create educational pathways for students that meet both academic standards and industry needs.