Chapter 10
A Cybersecurity Skills Framework

Peter James Fischer
Institute of Information Security Professionals, UK

ABSTRACT

This chapter traces the evolution of cybersecurity skills requirements and development over the past 40 years, from the early days of computer security (Compusec) to the present day. The development of cybersecurity skills is traced from an initial focus upon national security and confidentiality through to the current recognition as business driver. The main part of the chapter concentrates on the development of a specific skills framework from the Institute of Information Security Professionals. Originally conceived in 2006 and initially used for purposes of membership accreditation, the IISP Skills Framework has since been used extensively by commerce, industry, government and academia in the UK and more widely. Version 2 of the framework was published in 2016, and the chapter discussion outlines both the original structure and the notable changes in the later release. These developments collectively illustrate the ongoing recognition of cybersecurity skills, as well as the evolution of the skills themselves.

INTRODUCTION

The content of this chapter is based on the evolving requirement for identifiable, specific and measurable skills in cybersecurity disciplines to enable organizations to identify the range and blend of skill sets they require to secure their business and to gain assurance that the individuals employed to deliver the required cybersecurity services are competent to the required level. As a corollary to this, individual cybersecurity professionals need to be able to measure themselves against an appropriate subset of cybersecurity skills in order to deliver effective cybersecurity services to their employer or customer.

The Institute of Information Security Professionals (IISP) Skills Framework was developed to identify the range of cybersecurity skills needed in the modern business world and provide some criteria against which practitioners could measure the level of their skill. It is used as the main focus for describing cybersecurity skills and knowledge. However, it should be recognized that other frameworks have been developed and are in common use, most notably those developed by ISC^2 and ISACA. In

DOI: 10.4018/978-1-6684-3554-0.ch010

terms of knowledge, the Cyber Security Body of Knowledge (CyBOK) Project sponsored by the UK National Cyber Security Centre (NCSC) will enhance further the knowledge standards and criteria for cybersecurity professionals.

However, it was felt that it would be useful to provide some historical perspective on the development of, and the need for, cybersecurity skills over the past 40 years or so. In doing so, the modern term 'cybersecurity' has been used throughout, although different terms were used at the time, including Computer Security (Compusec), Data Security, Information Security (Infosec) and Information Assurance (IA). There is a strong UK focus in the text, but reference is made to seminal work in the USA and also within Europe which has influenced and contributed to the UK positions.

BACKGROUND

In this section, we cover cybersecurity perspectives from the 1970s to the early 2000s, showing the changes in skill requirements.

The Early Days: Confidentiality Is King

Research by David Bell and Leonard LaPadula in the 1970s, building on work by Ware (1967), resulted in the Bell–LaPadula Security Model (Bell and LaPadula, 1973; Bell and LaPadula, 1976). This was used as a basis for the US Trusted Computer Security Evaluation Criteria (TCSEC), commonly referred to as 'The Orange Book'. TCSEC was issued by the US National Computer Security Center (NCSC) in 1983 and published as a Department of Defense Standard in 1985. Its focus was unashamedly the protection of confidentiality, based on national security classifications and labels and, as such, became the benchmark for government security in both the UK and US during the late 1980s.

TCSEC utilized four categories of security functionality and assurance (DoD 1985):

D: Minimal protection, reserved for products which had failed evaluation at a higher level
C: Discretionary Protection (C1 and C2)
B: Mandatory Protection (B1, B2 and B3)
A: Verified Protection (A1)

The rigor of the development and evaluation processes were linked to the functionality levels, i.e. C1 systems possessed relatively limited security functionality and assurance, whereas A1 systems possessed finely-defined security functionality combined with rigorous standards for development and evaluation, including formal methods.

A range of supporting standards and guides were published by the US National Computer Security Center (NCSC) during the period 1988-1995. These were published with covers in different colors and were known as the 'Rainbow Series'. Arguably, the most notable of these were the Trusted Network Interpretation (TNI) and the Trusted Database Interpretation (TDI) published with red and purple covers respectively, although the color purple was also used for guides on the procurement of trusted systems.

Under the regime of TCSEC and the Rainbow Series, the need for cybersecurity skills, as defined in the IISP Skills Framework, was restricted more or less to Security Architecture, Secure Development and Security Evaluation plus, on the user side, Security Policy and Standards. There was little scope