Chapter 5
The CyberSecurity Audit Model (CSAM)

Regner Sabillon
Universitat Oberta de Catalunya, Spain

ABSTRACT

This chapter presents the outcome of two empirical research studies that assess the implementation and validation of the cybersecurity audit model (CSAM), designed as a multiple-case study in two different Canadian higher education institution. CSAM can be applied for undertaking cybersecurity audits in any organization or nation state in order to evaluate and measure the cybersecurity assurance, maturity, and cyber readiness. The architecture of CSAM is explained in central sections. CSAM has been examined, implemented, and established under three research scenarios: (1) cybersecurity audit of all model domains, (2) cybersecurity audit of numerous domains, and (3) a single cybersecurity domain audit. The chapter concludes by showing how the implementation of the model permits one to report relevant information for future decision making in order to correct cybersecurity weaknesses or to improve cybersecurity domains and controls; thus, the model can be implemented and sufficiently tested at any organization.

INTRODUCTION

Organizations try to protect cyber assets and put into effect cybersecurity measures and programs, however in spite of this continuing effort it is far unavoidable to avert cybersecurity breaches and cyberattacks.

A recent study from Hiscox (2017) highlights that prevalence of cyberattacks is high in British, American and German Companies from unique industries and sectors together with technology, financial, enterprise services, manufacturing, professional services, retail, construction, transport, food and drinks, healthcare, leisure, telecommunication, real estate, media, energy and pharmaceutical and starting from small organizations to large corporations; 57% of the corporations have experienced as a minimum one and 42% of those corporations have dealt with two or more cyberattacks within a year. Most businesses (62%) usually get over a cyber incident in much less than 24 hours; a quarter (26%) usually takes less than an hour to get back to business while some groups spend days or more to recover

DOI: 10.4018/978-1-6684-3698-1.ch005

from a cyberattack. A current trend covers greater spending in cybersecurity budgets, companies that already experienced a cyberattack are willing to put money into acquiring prevention technologies (24%) and detection technologies (23%). Smaller organizations incur with higher economic effect because of cyberattacks in comparison with larger corporations, most companies that participated in this study are taken into consideration as "cyber novices" in relation with the cyber readiness test (Hiscox, 2017) – the gap analysis indicates that investing money or having huge cybersecurity budgets do not help corporations to attain a "Cyber Experts" level. On the contrary, a major financial outlay isn't always the solution but enforcing other strategy and process measures like upper management involvement, cybersecurity awareness training, systematic monitoring and documentation. The costs of a cyberattack vary by geographic zones, for instance with corporations with more than 1,000 employees the financial impact will cost $ 53,131 in Germany, $ 84,045 in the UK and $ 102,314 in the USA.

Meulen et al. (2015) indicate that stakeholders need to comprehend the threat landscape in order to prepare for potential cyberattacks and at the same time to enforce defensive measures for protection. They summarized that there are not unique standards for classifying cyberthreats, the existing evidence suggests that is uncertain when it comes to defining threat assessments; they identified states, cybercriminals and hacktivists as the main threat actors and they also perceived cyberthreats linked to access, disclosure, manipulation of information, obliteration and denial of service.

In spite of enough cybersecurity measures, employees continue to be the weakest link in cybersecurity. Personnel are directly connected to financial losses related to data breaches and cybersecurity incidents (Pendergast, 2016).

IT audits are being redefined to include cybersecurity however there aren't clear guidelines or unison to which areas, sub-areas, domains or sub-domains to incorporate in a cybersecurity audit. The CyberSecurity Audit Model (CSAM) was designed to address the limitations and inexistence of cybersecurity controls to handle comprehensive cybersecurity or domain-specific cybersecurity audits. An comprehensive cybersecurity audit model is needed to support the information security function. Furthermore, a model to deliver cybersecurity awareness training based on company roles is also necessary to change the traditional awareness programs.

We present the results of two empirical studies that assessed the implementation and validation of the CSAM through extensive cybersecurity audits. These studies were motivated by the lack of universal guidelines to conduct comprehensive cybersecurity audits and the existing weaknesses of general programs to deliver cybersecurity awareness training.

Our multi-case studies were conducted to answer the following questions:

How can we evaluate and measure the cybersecurity assurance, maturity and cyber readiness in any organization or Nation State?

Why it is necessary to increase cyber awareness at the organizational and personal levels?

BACKGROUND

This chapter look into an innovative model for creating, developing, planning, delivering and maintaining a CyberSecurity Audit (CSA) methodology or program that was corroborated in two different Canadian Higher Education organizations under unrelated projects and schedules. The implementations in both organizations were part of a multi-case study research along with the Cybersecurity Awareness TRAining Model (CATRAM); another innovative model to conduct and deliver cybersecurity awareness training.