Chapter 17
Building a Maturity Framework for Big Data Cybersecurity Analytics

Chi Minh Pham
Deakin University, Australia

ABSTRACT

In recent years, big data analytics has become widely applied in cybersecurity, leading to the novel approach of big data cybersecurity analytics. While some organizations have been adopting this new approach in tackling cybercrime, there are limited guidelines to which companies can refer. Therefore, the renowned maturity model concept, which offers a systematic approach for an organization to measure and improve its maturity level, is applied in this study. On the basis of a comprehensive literature review, this chapter proposes a maturity framework for big data cybersecurity analytics. This synthesized comprehensive maturity framework comprises seven dimensions across five stage levels—namely organization, human, infrastructure, data management, analytics application, governance, and security dimensions. Knowing which dimensions need to be improved and which pathway to follow ensures the successful implementation of big data cybersecurity analytics within organizations.

INTRODUCTION

Despite advances in technology, cybersecurity may not become obsolete over time because these advances simultaneously enable modern cybercriminals to employ breakthrough techniques to damage organizations (Jegede, 2016; Matrane, Talea, & Okar, 2014), and breaches and attacks have increased across organizational levels ranging from industries to government agencies. Therefore, the modern era of information complexity has led to not only increased big data volume, where petabytes and exabytes of information are transferred daily, but also increased breakthrough cyberattacks (Mahmood & Afzal, 2013).

DOI: 10.4018/978-1-7998-8954-0.ch017

According to Mahmood and Afzal (2013), cybersecurity includes techniques, processes, and methodologies aimed at thwarting illegal attacks and protecting systems and networks from damage. Security analytics is a specific technique used to detect cybercrimes and measure cybersecurity performance on a large (national or international) scale (Cybenko & Landwehr, 2012).

Big data empower security analytics by supplying available data types for correlation and processing in analytics for security purposes (Shackleford, 2016). In addition to analyzing structured data, big data analytics operates with bunches of semi-structured and unstructured data (e.g., security data such as text in log files, security events, and GPS locations), which confer invaluable information. Hence, big data, characterized by the four Vs—volume, velocity, variety, and veracity—can solve the challenging questions on data limitations and data set availabilities for validation. When traditional techniques cannot handle the complexity of cybersecurity attacks and crimes, the big data approach is a potential solution.

However, big data cybersecurity analytics (BDCA) is substantially different from other types of security analytics. BDCA includes functions such as technologies for integrating dissimilar data types, ETL tools, multidimensional analysis, and advanced data visualization applications (Sullivan, 2015). However, there are many fundamental components that need more development, presenting problems ranging from human resources and investment to IT architecture for capturing and storing data.

With these scenarios, both practical and research sectors are in need of clear guidelines that present a road map for the future of big data application in cybersecurity. To solve the problem, this study proposed a maturity framework for BDCA with systematic guidelines and staged evolutionary levels. The maturity framework might encourage organizations to implement big data platforms and develop business strategies, while providing a complete picture of big data development, particularly for cybersecurity purposes. This may motivate researchers to continue the innovation or identify a related sub-field that warrants investigation.

For this purpose, a maturity framework to describe the significant steps in the maturity pathway, and the effectiveness measurements of deploying BDCA in organization contexts, was developed. In addition, the model was transformed into a questionnaire that serves as a diagnostic tool to identify problems as well as measure capability maturity in BDCA programs in an organization.

The research contributes to the theory by introducing a wide range of indicators for the maturity framework in the field, and by placing indicators in a hierarchical level. Meanwhile, as a practical contribution, it assists organizations in evaluating their current programs against an ideal BDCA approach, so that they can identify gaps for improvement, as well as standardize the performance with other organizations in the industry.

The remainder of this paper is structured as follows. The next section provides a review of the relevant literature. The third section explains the research methodology before presenting the literature findings. In the subsequent section, the maturity framework for BDCA is outlined, followed by the conclusion and proposals for further research.

BACKGROUND AND LITERATURE REVIEW

The objective of this research was to develop a framework that guides organizations to reach maturity in their big data analytics platform for cybersecurity purposes. Figure 1 shows the three components of the research—big data analytics, cybersecurity, and maturity model.