Chapter 59
Big Data Analytics Adoption Factors in Improving Information Systems Security

Marouane Balmakhtar
Northern Virginia Community College, USA

Scott E. Mensch
Indiana University of Pennsylvania, USA

ABSTRACT

This research measured determinants that influence the willingness of IT/IA professionals to recommend Big Data analytics to improve information systems security in an organization. A review of the literature as well as the works of prior researchers provided the basis for formulation of research questions. Results of this study found that security effectiveness, organizational need, and reliability play a role in the decision to recommend big data analytics to improve information security. This research has implications for both consumers and providers of big data analytics services through the identification of factors that influence IT/IA professionals. These factors aim to improve information systems security, and therefore, which service offerings are likely to meet the needs of these professionals and their organizations.

INTRODUCTION

Organizations rely on information systems to excel in business and in their relevant industries. Hence, proposing strategies and investigating new information systems are not only beneficial for creating healthy business organizations, but also for their long-term existence as solid organizations in the face of evolving security threats. According to Yen et al. (2013), using Big Data analytics helps detect these attacks by aggregating large and diverse datasets from various data sources and by conducting long-term historical correlations to incorporate a posteriori information of an attack in the network's history. Big Data analytics, which is an alternative to other security tools and mechanisms that can be provided on and/off of an organizations' premises, helps information technology/information assurance (IT/IA) professionals

DOI: 10.4018/978-1-6684-3662-2.ch059

tackle many modern threats facing organizations such as ransomware and advanced persistent threats. IT/IA professionals must keep exploring novel means to alleviate and contain sophisticated attackers in the Big Data era which is transforming the landscape of security mechanisms in the perpetual arms race of attack and defense.

Since the 1990s, it has been quite remarkable how fast Big Data analytics has grown (Chen, Chiang & Storey, 2012; Oghuma, 2013; Ramamurthy et al., 2008). Organizations have tried to create a competitive edge through leveraging their source of data in decision making for strategic intelligence purposes (Barney, 1991; Grant, 1996; Halawi, Aronson, & McCarthy, 2005; Bell, 2013). Big Data analytics is used to process multiple data sources of various data sets for the intention of improving problem identification and persuading critical management decision needs (Giura & Wang, 2012). Simply put, as Brynjolfsson, Hitt, and Kim (2011) indicated, organizations that stress decision making based on Big Data analytics have greater overall organizational performance and productivity.

The recent paradigm shift of security attacks against the technology infrastructure requires a serious look at the best possible means of leveraging Big Data analytics for the purpose of enabling security. Security of information has become more of a Big Data analytics problem where huge amounts of data are used to correlate, analyze, and mine information to identify useful patterns for creating knowledge and protecting existing technologies (Gartner, 2012). The big data analytics leverages tools and mathematical models using large amounts of data to improve an organization's technological infrastructure (Raja & Rabbani, 2014).

Security attacks against the technology infrastructure may target any information system in the organization, and without formulating an end-to-end picture of the overall security health of the infrastructure, threats may go undetected over long periods of time (Hurst, Merabti, & Fergus, 2014; Munirathinam & Ramadoss, 2014). This causes a flaw, which results by having a suite of local tools that manage their own specific information systems and the absence of a common repository where data is stored (Alhyasat & Al-Dalahmeh, 2013; Tankard, 2012). While Big Data analytics continues to gain ground in cyber defense inside many organizations (François et al., 2011; Giura & Wang, 2012; Microsoft, 2014; Ponemon, 2014; Yen et al., 2013), Big Data tools and data management techniques are evolving that can efficiently evaluate security threats while sustaining the volume and velocity of growing information systems data (Gupta & Jyoti; 2014). Big Data analytics is a tool that helps improve business intelligence, but prior research does not show how it can help improve security of an organization's information systems (Evers, 2014; Hawking & Sellitto, 2012; Yeoh & Koronios, 2010). In other words, Big Data analytics, as a source of knowledge to information security professionals, could help improve security of an organization's information systems. Previous research provides a series of examples where economic, modeling and empirical methods are combined to improve security decision making. These include studies of business intelligent decision making (Wieder & Ossimitz, 2013), decision support system for security investment (Beresnevichiene, Pym, & Shiu, 2010), predictive analytics in data mining (Lam, 2014), metadata and data quality perception (Shankaranarayanan, Even, & Watts, 2006), and human and technical factors (Beautement, 2013). But no study actually measures whether Big Data analytics can leverage its analysis to uncover insights from data sources that help discover security patterns and develop actionable insights to secure an organization's information system (Baldwin, Beres, Duggan, Cassa-Mont, Johnson, Middup, Shiu, 2011).

Chen et al. (2012) and Evers (2014) demonstrated that big data analytics is a tool that helps improve business intelligence, but no research exists to validate factors that enable the adoption of big data analytics to help improve an organization's security posture (Alspaugh et al., 2014; Chrun et al., 2008;