Chapter 73
Cyber-Security Intelligence Gathering:
Issues With Knowledge Management

Ezer Osei Yeboah-Boateng
Ghana Technology University College, Ghana

Elvis Akwa-Bonsu
Detectware, Ghana

ABSTRACT

Recently, KM has found applications in cyber-security. Though the actionable information gathered is intangible, they are used to improve knowledge sharing in organizations. Key cyber-security objectives are to prevent, detect and respond to threats. Using open-sharing of vulnerabilities and exploits, cyber risks could be mitigated through info-sharing. Cyber-intelligence is perceived as a process and a product, with outcomes being alerts that solicit explicit responses, leading to mitigation of possible threats. Using the Scrum approach, relevant articles and databases were reviewed, towards improving mitigation strategies. A virtual machine experiment utilized various tools to gather intelligence. Results from footprinting were used to design a KM-based Cyber-Intelligence Gathering model that incorporates Lewin's Change Theory. It is intuitive and serves as an effective mitigation strategy for most organizations, especially SMEs. The implication is that knowledge sharing could be harnessed to create a pool of mitigation resources for most enterprises in developing economies.

INTRODUCTION

All attacks follow certain stages. By observing those stages during an attack progression and then creating immediate protections to block those attack methods, organizations can achieve a level of closed-loop intelligence that can block and protect across this attack kill chain. (Sager, 2014, p. 1)

Knowledge Management (KM) techniques have found applications in all spheres in technology based organizations, and in recent times with cyber-security (Tisdale, 2015). In spite of the intangible nature

DOI: 10.4018/978-1-5225-5634-3.ch073

of the actionable information, often gathered from knowledge capturing activities, they can be employed to improve information sharing and management in organizations (Belsis, Kokolakis, & Kiountouzis, 2005). Managing enterprise networks require the use of knowledge management methods employed in the gathering of information, open-sharing of vulnerabilities and related exploits, as well as hotfixes from vendors.

Knowledge is defined as a "fluid mix of framed experiences, values, contextual information and expert insights … [which] is often embedded …. in documents or repositories [such as] organizational processes and practices" (Davenport & Prusak, 2000). Knowledge management is utilized in the collection, organization, analysis and collaborative sharing of the vast amount of information to the cybersecurity professionals, national security agents, and business community, etc.

Often, most IT professionals have perceived cyber-security as a mere technical problem. However, in recent times researchers are highlighting that a holistic cyber-security endeavors involve business concerns, governance and compliance issues, as well as organizational psychology (Tisdale, 2015) (Yeboah-Boateng, 2013a).

As businesses utilize the opportunities offered by ICTs, they are also exposed to cybersecurity challenges, such as vulnerabilities and threats. These vulnerabilities are flaws and weaknesses, which are typically inherent within the systems design, configurations and operations (Yeboah-Boateng, 2013a). When these susceptibilities are not properly dealt with, they can be exploited by various threats. "Whenever they are attacked [businesses] are adversely affected by way of loss of revenues, loss of customer confidence, loss of investor confidence, loss of resources, loss of credibility, cost related to dealing with the security breaches, cost of mitigation, as well as possible business closure, etc." (Yeboah-Boateng, 2013a, p. 1).

In 2014, for example, studies uncovered that major vulnerabilities, known for many years, which had been dormant were then being exploited. The situation was exacerbated as those exploited breaches in turn facilitated other possible intrusions or incidents (Bradley, Alvarez, Kuhn, & McMillen, 2015). In essence, vulnerabilities – be they unknown or undisclosed or undiscovered – there must be best efforts employed to limit the extent of impact in the event of incident or attack.

In cyber-security related endeavors, the quality of data validation and dissemination of the information gathered are key. There's the need to exchange information in managing vulnerabilities (such as Day-Zero vulnerabilities), threats, incidents, etc. (Dandurand & Serrano, 2013). Generally, KM analytics can be used for effective management of these actionable information in mitigating the possible risks to the organizations. Aspects of KM lend their support to cyber-security management, including information gathering on vulnerabilities and associated patches, data analytics, collaboration and information sharing (Forbes & Ahmed, 2011).

In today's ubiquitous business environments, information sharing raises various concerns amidst social media and networks. How do organizations strike a perfect balance in sharing information and the need for real-time intelligence gathering? How does "Bring-Your-Own-Devices" (BYOD) impact on the knowledge management principles? What roles are users playing in knowledge management in respect of cyber-security? How are the user fulfilling their knowledge management roles in respect of cyber-security?

Using the Scrum methodology, we gleaned through extensive literature of key articles, databases, and authorities, towards improving the cyber-team's mitigation strategies, whilst minimizing the possibilities of exploitation (Yeboah-Boateng, 2013a). Typically, the agile development model requires extreme