Chapter 13
Integrating IS Security With Knowledge Management:
What Can Knowledge Management Learn From IS Security Vice Versa?

Murray Eugene Jennex
San Diego State University, USA

Alexandra Durcikova
Oklahoma University, USA

ABSTRACT

Knowledge management focuses on capturing and sharing knowledge. Because of this, KM researchers tend to focus on issues related to knowledge capture, storage, and sharing. However, because knowledge is valuable, it is a target needing to be protected. This chapter posits that KM researchers and practitioners also need to think about security and explores how important security skills are to KM practitioners and researchers. A literature review was performed to determine how much attention is paid by KM researchers to knowledge security. Additionally, KM job postings were examined to determine if security skills are considered important by those hiring KM practitioners. Next, a survey was prepared for exploring security attitudes of KM practitioners as an area of future research. Finally, future research areas for IS security are proposed that can greatly benefit from lessons learned in the areas of both knowledge sharing and knowledge sourcing.

INTRODUCTION

News reports have been reporting on several security breaches that either compromised the confidentiality of information and data stored in knowledge management systems (KMSs), availability of this knowledge, or its confidentiality. An example of the former is the Target breached with approximately in December 2013 when 40 million credit and debit card accounts exposed and financial and personnel data on up to 70 million customers accessed (Weiss and Miller, 2015). An example of the compromise of the

DOI: 10.4018/978-1-5225-5427-1.ch013

availability is the WannaCry ransomware that affected more than ten thousand computers in 36 hospitals and prevented medical staff from accessing vital patient information (Perlroth & Sanger, 2017). Finally, a recent spear-phishing prank (Tapper, 2017) that targeted some White House officials during summer of 2017 led to the disclosure of sensitive private information thus jeopardizing the confidentiality of it. While these examples my not be directly linked to a breach of a KMS, the magnitude and fall out from these massive security breaches also raises questions on the security of the knowledge stored in KMS. Information System (IS) security is about protecting IS assets, networks, data, information, computers, and applications by restricting access to the assets and preventing unauthorized modification or destruction. Knowledge management (KM) focuses on sharing and transferring knowledge from knowledge providers to knowledge users. It is not intuitive that security and KM are related as they have contradictory objectives: KM is about providing access to knowledge, while IS Security is about restricting access to knowledge. However, it is our position that KM and IS Security are complementary. While KM can be used to improve security performance, training and awareness (San Nicolas-Rocca, Schooley, & Spears, 2014), this chapter primarily focuses on the use of security in KM and touches on what IS Security can learn from KM. Knowledge has value and items of value are targets of theft and attack. This chapter posits that KM does not have close enough links with IS Security. It is posited that this is evidenced by not only a lack of research literature addressing the integration of KM and IS Security but also a lack of interest in integrating KM and IS Security by KM practitioners. To investigate the links between KM and IT Security this chapter performs a review of the KM research literature with respect to IS Security. Additionally, to assess how KM practitioners' value IS Security skills and capabilities KM job postings are analyzed to determine what skills and capabilities are desired in new KM position hires. Nest, we explore KM practitioner attitudes with respect to the role of IT Security in KM an exploratory survey is generated and presented in this chapter. Finally, before discussion, we touch upon papers that have already applied lessons learned from KM and KMS research into IS Security research.

The value of this chapter is in providing insight into perceptions and attitudes with respect to integrating IS Security into KM. The concern is that there is too little integration and that KM practitioners and researchers need to put more effort into creating secure KM and KMS. We believe this is necessary given the threat level in our cyber environment. As cyber threat is growing so is the cost associated with a breach. The Ponemon Cost of Cybercrime Report shows that the cost of data breeches has risen to an average cost of $8.9 million per breech in 2012, a 6% increase from 2011 (note that this is for the organizations in their survey) (Ponemon, 2012). The 2013 Ponemon Cost of Cybercrime report shows that the average cost per record breached rose from $188.00 in 2012 (Ponemon, 2013) to $2.3 billion USD annually according to the FBI (McCabe, 2016). In addition, the financial cost of a security breach, there is also the good will of all customers that is affected by it. Why then, as the case of Target breach illustrates, even if evidence of a breach is at hands, responsible managers don't take action? This chapter proposes that the lack of security awareness and knowledge by non-security practitioners, those practitioners responsible for sales, operations, and the performance of the organization; leads to poor security decision making. Our proposal is also supported by increased regulatory pressure on organizations to improve security awareness of their decision makers (Thune, 2017).

Finally, how are cyber-attacks carried out? While there is a variety of means, the most costly come from malicious insiders, web based attacks, and phishing attacks (Riecicky & Spichiger, 2012) with advanced persistent threats (APT) coming from state sponsored espionage (McWhorter, 2013) and sophisticated cybercriminal rings (Sophos, 2013). In addition, movement towards cloud and mobile technologies increases the reach of all of these threats. The cloud is increasing the use of service based