A Three-Vector Approach to Blind Spots in Cybersecurity

Mika Westerlund
Carleton University, Canada

Dan Craigen
Carleton University, Canada

Tony Bailetti
Carleton University, Canada

Uruemu Agwae
Carleton University, Canada

INTRODUCTION

With the increased use of network technologies (Clements & Kirham, 2010), cybercrime is on the rise. PricewaterhouseCoopers estimates that 120,000 cyberattacks occur daily (PwC, 2016). There is a need for cybersecurity throughout society. Cybersecurity is defined as "the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights" (Craigen, Diakun-Thibault, & Purse, 2014). It is also the measure of preparedness including recovery, protection, and triage against the losses caused by cyberattacks (Maughan, 2010).

Cybersecurity is key for protecting valuable assets such as intellectual property, virtual currencies, and industrial control systems (Kritzinger & Solms, 2010; Smith & Rupp, 2002). However, cyberattacks are often successful due to "blind spots," which refer to various biases and preconceived information that affects organizational and human decision making (Heuer, 1999; Pronin, Lin, & Ross, 2002), leading to unawareness of malicious activity (Boehm & Turner, 2005). It is important to understand how to mitigate all blind spots, particularly those that can lead to massive economic losses (Flowers, Zeadally, & Murray, 2013).

The objective of this chapter is to investigate eight cyberattack cases ("attack scenarios") from the viewpoint of "the core vectors" which include economic, technological and psychological perspectives to blind spots. While previous research has viewed core vectors in isolation from each other (Baker, 2014; Garfinkel, 2012; Singer & Friedman, 2014), this chapter focuses on how to mitigate blind spots in cybersecurity by using a holistic three-vector approach. The holistic view to cybersecurity has been suggested by many authors (Emami-Taba, Amoui, & Tahvildari, 2013; Hua & Bapna 2013; Hughes & Cybenko, 2013).

Section one provides an overview of cyberattacks and blind spots that enable attacks. Section two discusses core vectors conceptualized as psychological, economic, and technical perspectives to blind spots. Sections three and four discuss research methods and eight scenario cases. Section five presents a summary table of the cases included in the sample. Finally, sections six and

DOI: 10.4018/978-1-5225-2255-3.ch147

seven discuss future research avenues and implications to practice.

BACKGROUND

Han and Dongre (2014) list political, economic, and socio-cultural motives as primary motives for cyberattacks, and emphasize that attackers can be organizational insiders or outsiders. Political motives include cyber terrorism against foreign nations or multinationals (Hua & Bapna, 2013) and ethically fighting for justice and human rights (Gandhi et al., 2011). Other motives may be plain entertainment. Regardless, there is a propensity for harm when cyberattacks occur. Understanding what enables these attacks enables mitigation, and will contribute to the theory on blind spots in cybersecurity (Chen, Huang, Xu, & Lai, 2015; Nathan & Petrosino, 2003).

Blind spots are dangerous because they are about biases and preconceptions (Pronin et al., 2002). Humans tend to interpret new information so that prior conclusions remain intact. A 2012 survey by the National Cyber Security Alliance (NCSA) and Symantec revealed that 83% of small U.S. companies did not have a formal plan for keeping their business cyber-secure although over 70% responded that a safe and trusted Internet is critical to their day-to-day operations. A total of 76% thought that their company was safe from cyber-security breaches.

Given that blind spots are inevitable, there is a need to develop more efficient means to mitigate them. Thus, it is critical to understand how (i) the business, (ii) the psychological, and (iii) the technological perspectives might help organizations and individuals to recognize and avoid blind spots. This core vector thinking is supported by the cybersecurity assessment factors by Gavins and Hemenway (2010) and the categorization of attacker motivations by Han and Dongre (2014). Combining vectors enables a comprehensive analysis of past cyberattack scenarios in order to mitigate blind spots.

PERSPECTIVES TO CYBERSECURITY

C

Cybersecurity should be examined through psychological, economic, and technological vectors. Wiederhold (2014) argues that psychology in human nature is the weakest link in cyberspace. Although technology is sophisticated, humans still fall victim to social engineering (Bauer & van Eeten, 2009). Economic factors are important as computers are infested with malware to enrich attackers, and victims ponder associated costs (Hua & Bapna, 2013).

Psychological Vector

Human factors affect cybersecurity the most (Baker, 2014), and when cyber threats are not understood or are ignored, adverse consequences accrue. What people perceive of risks affects how they behave (West, 2008). The 2012 NCSA/McAfee survey showed that 64% of Americans feel their smartphone is safe from cyberattacks even though they had not installed any security software.

Sukamol and Markus (2008) argue that many individuals make security decisions from a simplistic understanding of risk. In organizations, risk has focused on technology, but firms are now expanding their technology-centered perspective to include people and processes (PwC, 2016). Heuer (1999) notes that it takes more information and more unambiguous information to recognize an unexpected phenomenon than an expected one. Moreover, Cebula and Young (2010) argue that many people use the same combination of user ID and password for different information systems because of human memory limitations thereby creating a huge risk to cybersecurity.

The psychological vector is associated to human thinking and cognitive limitations affecting decision making. Humans are especially prone to blind spots when it comes to complex systems like law, politics, or cyberspace. A typical user may not be able to identify an email phishing attack or