Chapter 4
Cyber Attacks, Contributing Factors, and Tackling Strategies: The Current Status of the Science of Cybersecurity

Samantha Bordoff
University at Albany (SUNY), USA

Quan Chen
University at Albany (SUNY), USA

Zheng Yan
University at Albany (SUNY), USA

ABSTRACT

This article describes how as access to the Internet has increased, cybersecurity has become important, with businesses and the government spending much time and resources to combat cyber attacks. The purpose of this article was to review the existing literature related to cybersecurity. Specifically, the review synthesizes the empirical research in (1) various types of cyber attacks, (2) contributing factors related to cybersecurity behavior, and (3) strategi to improve cybersecurity behavior. The most developed line of research in this area has been focusing on the strategies to improve cybersecurity behavior, showing a questionable trend of quickly creating solutions before fully conceptualizing the problem.

INTRODUCTION

As Internet technologies become more ubiquitous throughout societies the threat of cyber attacks and the need for cyber security becomes even more important. Today, people access to the Internet from their pockets or backpacks by having wireless technologies such as smartphones and tablets that are able to

DOI: 10.4018/978-1-5225-7912-0.ch004

access wireless networks almost everywhere. However, for Internet technologies used in cyberspace, as with almost all new technologies, along with the good comes some bad.

Cyber attacks, an attempt to hack into or otherwise disrupt or destroy computer networks or other Internet devices, are one of the prominent negative outcomes to occur from this boom in Internet technologies (Bedser, 2007). A cyber attack could range from something as minor as an individual downloading a computer virus, to something as major as entire multinational corporations being hacked in order to gain insider knowledge or steal financial information from customers. Cyber attacks can lead to a person's identity or financial information being stolen and to small businesses going out of business due to the results of these attacks.

Cybersecurity is not a new research topic, but it has been a major national challenge for over 20 years and led to a rapid growth of the research literature in the past 10 years (e.g., Clark, Berson, & Lin, 2014; CSTB, 2002; USEOP, 2010 & 2011; USOWH, 2009). Since 1991, the Computer Science and Telecommunications Board (CSTB) of the National Research Council alone has produced seven major research reports, recognizing cybersecurity as a national challenge and summarizing various types of technical and nontechnical strategies to meet the challenge. However, in 2002, after 10 years of work on cybersecurity, CSTB stated that "there is a deep frustration that research and recommendations do not seem to translate easily into deployment and utilization" (CSTB, 2002). In 2014, after 20 years of work on cybersecurity, CSTB reported that "relatively little progress has been made in cybersecurity despite the recommendations of many reports from the Academies and elsewhere, and potential policy responses" (Clark, Berson, & Lin, 2014).

Given the fast-growing literature and the existing challenges in cybersecurity, the motivation of the current review article is to synthesize the current literature for researchers, policy makers, practitioners, and even general public. The first and the most systematical literature review was published in 2006 by Cannoy, Palvia, and Schilhavy, three scholars from North Carolina. In this review, Cannoy, Palvia, and Schilhavy searched the existing literature published between 1996-2005 in top journals in the field of information system and located 82 articles for their review. Specifically, they identified nine major areas focused in the existing literature (e.g., legal issues, monitoring and morality, vulnerabilities and risks, and detection) and developed a thoughtful framework to theorize major constructs and their relationships for the information system security research. This important review has made strong contributions to cybersecurity research by synthesizing the existing literature and presenting a comprehensive framework.

Built upon and motivated by this important review, the present review is intended to make new knowledge-synthesis contributions to cybersecurity research in three aspects. First, we searched the current literature between 2005-2015 to provide an update after the Cannoy, Palvia, and Schilhavy review between 1996-2005. Second, we expanded the literature search from information system security in specific to cybersecurity in general, including personal cybersecurity, business cybersecurity, and government cybersecurity, in order to develop a big picture of the current cybersecurity research. Third, we developed a broad framework that synthesizes the current cybersecurity literature by focusing on three sequentially interconnected major topics, that is, various cyber attacks, various factors contributing to cyber attacks, and various strategies to tackle cyber attacks.