# Chapter 11
# The Cyber Acumen:
## An Integrative Framework to Understand Average Users' Decision-Making Processes in Cybersecurity

**Xiang Michelle Liu**
*Marymount University, USA*

## ABSTRACT

*The major purpose of this chapter is to understand average user's decision-making process in cybersecurity by reviewing and integrating several major theoretical frameworks discussed and applied in decision making processes in cybersecurity. The average users are the ones who do not realize or understand when or how to perform security-critical decisions, the ones who are unmotivated to comply with company and school cybersecurity policies and procedures due to inconvenience, and the ones who do not have sufficient knowledge in cybersecurity to make sound security decisions. It is important to discuss and understand the role of such users and their behaviors based on systematic analysis so that we can identify potential factors causing "poor" security decisions and find ways to reduce the likelihood of being victims of cyber-attacks. The ultimate goal is to provide insights and make recommendations on how to foster individual's cyber acumen and cultivate a more effective decision-making process.*

DOI: 10.4018/978-1-5225-7128-5.ch011

# INTRODUCTION

*Only amateurs attack machines; professionals target people. (Schneier, 2015)*

## Background

Juniper Research predicted that rapid digitization of consumers' lives as well as organizational and government records will increase the cost of cybercrimes to $2.1 trillion globally by 2019, quadrupling the estimated cost of cybercrimes in 2015 (Juniper Research, 2015). Another report released by the Centre for Strategic and International Studies (CSIS) disclosed that, in the U.S. alone, cybercrime caused the loss of at least one half million jobs annually as companies struggle with the loss of intellectual property and suffer reputational harm (Center for Strategic and International Studies, 2013). According to the FBI's Internet Crime Complaint Center (IC3), a federal agency providing the public with a reporting system and monitoring trending scams, significant amount of complaints were filed by the public in 2016 centered around business email compromise (BEC), ransomware, tech support fraud, and extortion (Internet Crime Complaint Center, 2017). The report disclosed that among various types of cybercrimes, the top three crime types by reported loss were BEC, romance and confidence fraud, and non-payment and non-delivery scams; while the top three crime types reported by victims were non-payment and non-delivery, personal data breach, and payment scams in 2016. IC3 received a total of 298,728 complaints with reported losses in excess in $1.3 billion in 2016 alone.

Hundreds of thousands of people fall victim to cyber attacks and cybercrimes each year, ranging from a local Virginia supermarket phished by an individual posing as the company founder (see Bryan, 2017) to the Anthem data breach started by a phishing campaign and ending with 78.8 million consumers' personal data potentially exposed (see Snell, 2017). Cybercriminals have been persistently engaged in exploiting vulnerabilities known and/or unknown to the public, from various devices, networks and systems. More often, they succeed by taking advantage of inherent natures or weakness of human beings such as curiosity, credulousness, wanting to be helpful, greed, and trading security measures for convenience. For instances, as early as 2000, ILOVEYOU letter virus quickly swept through banks, securities firms, and tech companies worldwide by luring users to open an email with the subject line ILOVEYOU and download attached files with virus embedded (see Strickland, 2018). As almost two decades passed since ILOVEYOU spreading, it is becoming