Understanding the Relationship Between Cybercrime and Human Behavior Through Criminological Theories and Social Networking Sites

5

Anne-Marie Mohammed
The University of the West Indies, St. Augustine, Trinidad and Tobago

Vladlena Benson
Aston Business School, UK

George Saridakis
University of Kent, UK

INTRODUCTION

Social networking sites (SNS) are, "applications that enable users to connect by creating personal information profiles, inviting friends and colleagues to have access to those profiles, and sending e-mails and instant messages between each other" (Kaplan and Haenlein, 2010:63). Any type of information such as blogs, photos, videos and audio files can exist within these personal information profiles. Therefore, SNS can be viewed as virtual communities that enable on-demand communication and interaction with real-life friends as well as the ability to meet new friends from around the world based on similar interest (Kuss and Griffiths, 2011). The rapid growth in usage of SNS worldwide in recent years, permits its description as a 'global consumer phenomenon' (Kuss and Griffiths, 2011). While there are great advantages for the use of SNS, one research by Kuss and Griffiths (2017) suggests that constant usage can create the perception of a need to be online. This may result in compulsive and excessive use of SNS and in some cases give rise to symptoms associated with substance-related addiction. This excessive use of SNS can reduce the productivity of users as well as increase their exposure to cyberattacks. On the other hand, a recent study by Allcott et al. (2019), explores the welfare effects of SNS and discovers that the majority of their sample value access to SNS for four weeks is at US $100 or more. Therefore, this valuation suggests that consumer surplus for SNS is expected to be in the billions of dollars considering the large number of active users globally. According to Pew Research Center (2018), Facebook and YouTube are the most popular SNS among adults whereas Snapchat and Instagram are the most popular among young adults. Facebook is by far the most popular social networking site globally with 1.52 billion active daily users and 2.32 billion active monthly users (Facebook, 2018).

SNS have become the mainstream communication medium for individuals, especially young people (Holt and Bossler, 2014), and businesses (Culnan et al., 2010). At present there are approximately 4.17 billion internet users worldwide, thus demonstrating a sustained growth from the year 2015 by a quarter. Of these, 3.4 billion are active social media users with a similar proportion of mobile internet users (3.7 billion) according to Statista (2018). However, with the continuous loss of control over personal information that is exposed online, individuals and businesses present easy targets for non-technical attacks

DOI: 10.4018/978-1-5225-9715-5.ch066

ranging from spear-fishing to whaling leading to serious cyber victimization (McAlaney et al., 2018). Cybersecurity professionals agree that this security depends on people more than on technical controls and countermeasures. Recent reviews of cyber security express that no industry sector is invulnerable to cyber-attacks and that the public sector tops the list for targeted security incidents (Benson, 2017). This is largely attributed to the weaker cyber security mind-set of employees. On the other hand, the financial sector, year on year, experiences the highest volume of cyber breaches. These are predominantly aimed at financial gain or espionage. What is common among these rather different sectors is that the attack vector by cyber criminals starts with social engineering. The weakest link in the security chain is still the human element. Irrespective of the market segment, the losses contributing to the current global cost of cybercrime are huge with an estimation of approximately $600 billion (McAffee, 2018).

Unsurprisingly, the human behavior in an online context has been addressed by researchers for some time. The cybersecurity industry, policymakers, law enforcement agencies and public as well as private sector organizations are yet to realize the factors affecting the risk of online victimization and the impact on individuals and businesses (Taylor et al., 2010). In order to improve cybersecurity practices, there is a need for a discussion acknowledging that cybersecurity is inherently a complex socio-technical system.

This chapter presents an overview of emerging issues in the psychology of human behavior and the evolving nature of cyber threats. Theories of crime and empirical studies on user victimization as seen on social networks are reviewed. The chapter reflects on the role of social engineering as the entry point of many sophisticated attacks and highlights the relevance of the human element as the starting point of implementing cyber security programs in organizations as well as securing individual online behavior. There are numerous theories of crime that are relevant and applicable to cybercrime. However, this chapter focuses specifically on the routine activity theory (RAT) put forward by Cohen and Felson (1979) and the general theory of crime (GTC) introduced by Gottfredson and Hirschi (1990). These have relevance since the GTC is the most eminent latent trait theory of crime (Siegel, 2006) and the RAT gives a sociological explanation aimed at crime events rather than criminal propensities (Schaefer and Mazerolle, 2017), thus making both theories interesting and suitably applicable to cybercrime. This chapter also mentions the rational choice theory (RCT) as well as the deviant place theory (DPT) but to a lesser extent simply touches on some of the other existing theories of crime. For example, Cohen and Felson (1979) argue that crime will occur when there is a motivated offender, a suitable target/potential victim and the absence of guardians capable of preventing any violation. The latter can be in the form of physical guardianship (e.g. antivirus) or personal guardianship (e.g. computer skills). In addition, Gottfredson and Hirschi (1990) suggest that crime and victimization are associated with low levels of self-control. We then turn to empirical studies that have examined the user behavior on SNS leading to victimization (e.g. Hansen et al., 2017; Saridakis et al., 2016; Benson et al., 2015a-c). Issues associated with the emerging trends in human behavior research and ethics are presented for further discussion. The chapter concludes with a set of open research questions warranting immediate academic attention to avoid the exponential growth of future information breaches.

BACKGROUND: THEORIES OF CRIME

Research suggests that the frequency of internet usage shares a positive association with cyberbullying and victimization (Mesch, 2009). However, in modern times, most individuals, public organizations and private ones are heavily dependent on the usage of the internet to carry out their daily business activities and communications, therefore, limiting internet use is not a plausible solution to the problem of being