International Journal of Cyber Warfare and Terrorism
Volume 10 • Issue 1 • January-March 2020

Terrorism Effects on Businesses Post 9/11

Mariah Talia Solis, University of Tampa, USA
Jessica Pearson, University of Tampa, USA
Deirdre P Dixon, University of Tampa, USA
Abigail Blanco, University of Tampa, USA
Raymond Papp, University of Tampa, USA

ABSTRACT

Discussions regarding terrorism are more relevant today than ever before. Terror threats can take on many forms from physical violence against military forces, individual companies, and ordinary citizens, to actions against infrastructure, to cyber terrorism. These forms of terror and others, in a number of ways, threaten the physical and financial safety of people around the world. The purpose of this qualitative research study is to evaluate the effects of terrorism—particularly the attacks on September 11, 2001—on U.S. enterprises in the period since the attacks. Utilizing interviews with representatives from various industries, the authors found that employees with long company histories believe their companies have implemented changes regarding their security measures as a safeguard against possible future terrorist attacks. The research findings revealed that while businesses have made changes in their use of technology to change their (1) cybersecurity, (2) training methods, and (3) hiring processes, there remains a gap in understanding the efficacy and efficiency of these changes. Though the September 11 attacks raised the concerns regarding terrorism overall and formed the genesis for thinking about the effects of terrorism, the authors found that interviewees had limited knowledge of how terrorist activities truly affected their business, and identified a strong need to empirically study the technology changes implemented in the past two decades as a response to terrorism, and a need for a thorough sharing of knowledge within the cybersecurity industry to other businesses.

KEYWORDS

9/11, Al-Qaeda, Cybersecurity, Hiring, Military, Qualitative, Terrorism, Training

INTRODUCTION

Terrorism is not a new phenomenon. The conquest of Judah and the use of terror tactics by Nebuchadnezzar and the Babylonians is well documented (Forst, 2009). Arguably, the American militia in the revolutionary war used “terrorist” techniques against the British forces (Tilly, 2017). In modern times, groups such as Al-Qaeda, the Taliban, and the Islamic State in Iraq and Syria (ISIS) have become symbols of foreign terrorist groups. In the United States, domestic extremists groups such as Antifa, the Ku Klux Klan (KKK), the Atomwaffen Division, the Democratic Socialists of America, and several others have been labeled as terrorist organizations (Chermak & Gruenewald,

DOI: 10.4018/IJCWT.2020010102

2015; LaFree, 2018; Perliger & Sweeney, 2019). Between 1970 and 2018, the Global Terrorism Database (GTD) has recorded some 126 terrorist incidents on U.S. soil aimed at government, media, and businesses as well as private citizens and property ("Global Terrorism Database," 2019).

Organized groups are not the only threat. The use of social media to radicalize individuals into extremist groups of many varieties generates further concern (D'Souza, 2018). The growth of technology has allowed individuals with skills, knowledge, and relatively inexpensive computer equipment the power to disrupt businesses and societies. Concerns over "lone-wolf" attacks (attacks by individuals with no command from, or even a connection to an organized group) remain. The decentralization of the "enemy" to attack has caused challenges to the ability to protect businesses and society from terrorist attacks (Phillips, 2017).

September 11, 2001 changed the platform for national security and terrorism procedures in the United States. The attacks catapulted terrorism into the national consciousness, sparking massive government agencies like the Transportation Security Administration (TSA) and the larger Department of Homeland Security (DHS). Within the U.S., the attacks also led to restructuring of the Federal Bureau of Investigation (FBI) (Reedy & Miller, 2016) and highlighted the desperate need for the flow of communication and information among federal, state, and local governments, emergency responders, hospitals, transportation agencies, and private sector businesses such as utilities. The attacks ultimately led to the ongoing Global War on Terror.

The national security sector was not the only segment of the economy to experience changes as a result of the attacks. A variety of businesses, from healthcare to aviation, saw the attacks as a possible harbinger of things to come. They sought to examine and update their security procedures as a result. Companies began to implement changes to their mass casualty and safety procedures. Some firms began to engage or pursue increased engagement in threat mitigation training (Ahmed, Suarez, & Andreychuk, 2019).

The attacks ultimately lead to the ongoing global war on terror, with formal conflicts occurring in Iraq and Afghanistan, creating the need for greater global coordination and communication on the part of the U.S. military and firms working with them. These global requirements echoed and amplified the necessity for communication and coordination between federal, state, and local governments, as well as the coordination and communication between government and private businesses. These needs, combined with the explosive growth in technology, have driven private industry to recognize cybersecurity as a preeminent requirement of their businesses.

Our research aims to fill a gap in the current understanding of the impacts of terrorism post-9/11. In particular, we look to evaluate the effects of the terror attacks in 2001 and the subsequent changes on U.S. businesses. After conducting interviews with individuals from various industries, we conclude that companies have implemented changes, primarily in three areas: (1) cybersecurity, (2) changes in training, and (3) changes in hiring practices. Although the September 11 attacks raised concerns regarding terrorism overall, interviewees had very limited knowledge of terrorist activities and the actual impact of these events on their industries. In addition, the study identified a strong need for an empirical evaluation of cybersecurity methods and a thorough sharing of knowledge and a risk/benefit/cost analysis to other private sector businesses regarding their technological and cybersecurity budgets.

BACKGROUND

On the morning of September 11, 2001, 19 Al-Qaeda operatives carried out a series of four coordinated attacks in the United States. Boarding domestic aircraft, each stocked with fuel for cross-country flights, the groups hijacked each plane shortly after takeoff. Within just a short time, two of the planes crashed into the north and south towers of the World Trade Center (WTC) in New York City while the third was flown into the Pentagon just outside of Washington, D.C. The fourth, final plane crashed in a Pennsylvania field after passengers thwarted the plans of the terrorists— at the cost of

A Steganalytic Scheme Based on Classifier Selection Using Joint Image Characteristics

Jie Zhu, Qingxiao Guan, Xianfeng Zhao, Yun Caoand Gong Chen (2020). *Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications (pp. 362-376).*

www.irma-international.org/chapter/a-steganalytic-scheme-based-on-classifier-selection-using-joint-image-characteristics/251437