Chapter 1
Business Resilience in a Cyber World:
Protect Against Attacks Part 2

Sharon L. Burton
https://orcid.org/0000-0003-1653-9783
Capitol Technology University, USA

ABSTRACT

This chapter examines the shift from business impact analysis to the business resilience required to safeguard organizations from cyber-attacks and endure such attacks if they befall. Skilled business resilience experts support accepted practices that enhance efficiencies and quality of business continuity strategy and planning programs, plus guard against cyber terrorism. Via this text's pages, readers learn about resilience as the final critical planning, preparative, and related action recommended to substantiate that organizations' significant business functions should either persist to function despite serious cataclysms or events of cyber terrorism that otherwise might interrupt services or production or will be recovered to an operational state within a reasonably short period. Explored is evidence of the ubiquitous reliance on technology in business strategies. Shown is how business resilience procedures provide an array of advantages. Readers will learn about business resilience as a long-term solution and business resilience cyber-risk management strategies.

INTRODUCTION

This study aims to analyze the business resilience of Sigma Pointe that supports the organization and then identify what businesses do to build business resilience within their organizations. Sigma Pointe's current "as-is" state is that the researcher does not have a framework or model for providing a business resilience strategy. Nor does this researcher have a framework or model for standing up the business resilience strategy office. Further, the most current directive specifies that Sigma Pointe shall employ the critical capabilities to copiously institutionalize continuous process improvement, specifically business

DOI: 10.4018/979-8-3693-1906-2.ch001

resilience, within its organization. The initial work was to gather end-to-end data regarding business resilience.

Before 2001, business continuity plans were habitually propelled by threats from natural disasters. The events of 2001 were momentous. Experienced was the 2001 terrorist attack on the World Trade Center in New York City. The top five costliest hurricanes are (i.e., Katrina, 2005, $165 billion; Harvey, 2017, $127 million; Maria, 2017, $91 million; Sandy, 2012, $72 million; Irma, 2017, $50 million; Pompa, 2018). The top five earthquakes are Nepal, 2015, with a magnitude of 7.8; Italy, 2016, with a magnitude of 6.2; Indonesia, 2016, with a magnitude of 6.4; Mexico, 2017, with a magnitude of 7.1; Japan, 2011, with a magnitude a 9.5; Noonan & Wires, 2018). Other disasters such as cyber warfare attacks (e.g., Google China hit by a cyberattack - 2009; Scientology attached by hackers – 2008; Internet attack on all 13 domain name systems' root servers in the United States – 2002; hacker Gonzales steals tens of millions in credit card details - 2009; ARN Staff, 2019) Since these catastrophes a change occurred. Businesses began asking whether their organizations would survive (Updegraff, 2011). Businesses recover five years after these disasters (Forgany, 2022; Homeland Security Today, 2022; Lynn, 2022; Poole & Carithers, 2022; Schuppe, 2022; and Walker, 2022). The old question is - what is the time to recover operations? - does not allow for the broadest information gathering regarding business continuity (Updegraff, 2011). The Department of Homeland Security, created in November 2002 due to Congress's passage of the Homeland Security Act, further coordinated and united national homeland security work (Department of Homeland Security, 2019, Department Creation). This department opened on March 1, 2003, as a stand-alone, Cabinet-level department. This department transfigured and readjusted wholly or a portion of 22 different federal departments' and agencies' pursuits (Department of Homeland Security, 2019, Who joined DHS) into one department whose chief work remains to safeguard the United States of America (Department of Homeland Security, 2019, Proposal to Create). This change increased the threats the US government pursued to diminish and prepare to eliminate (Department of Homeland Security, 2019, Department Creation). Let us briefly review business continuity planning, a topic covered in a different publication.

Business continuity planning affects large, medium, and small businesses (Castillo, 2004) and drives through business impact analysis. The disaster recovery plan leads to understanding prioritization, planning, and preparing significant business functions for continued operations, notwithstanding grave disasters or incidents of cyber terrorism that interrupt services/production (Hatton et al., 2016). Cyber-terrorism is a chief concern because users have misused vulnerabilities from the early 90s to gain unlawful entry to networks for malevolent intentions (Dawson, 2015, p. 1). Notionally and qualitatively, disaster is recognized to disturb expansion through various conduits: haphazard occurrence, weak institutions, and voids in social safety nets, in addition to the short-termism of business leaders' policymaking practices. These conduits are several of the factors that propel natural disaster risk. A well-developed business continuity plan can serve to aid in the deterrence or decrease the risk of a cyber-attack; however, more planning and practice are needed. First, let us review business continuity.

Business continuity is a defined set of planning, preparatory, and related activities proposed to confirm that a business' significant operational functions will either continue to operate notwithstanding grave disasters or incidents of cyber terrorism that otherwise have interrupted services, production, or technology will be recovered to an operational state within a reasonable short period (Păunescu et al., 2018). Leaders must understand the recovery time objective (RTO) required for systems, networks, computers, and applications. RTO is the amount of targeted time an organization has to reestablish its practices and procedures at their prescribed suitable service level following a tragedy to circumvent unbearable