Chapter 57
Organizational Resilience Approaches to Cyber Security

David Gould
City University of Seattle, USA

ABSTRACT

This article includes a perspective on cyber security through the lens of the World Economic Forum Resilience Framework. As cyber threats are a continual threat to organizations, it may be useful to consider resilience as a complementary approach to technological responses. The problem is that organizations cannot generate a sufficient number and types of responses to cyber security threats as the number of threats and associated costs continues to increase. The purpose of this article is to explore some possible practices and approaches to counter the ongoing and escalating cyber security threats, with the understanding and wisdom that not all threats will be possible to stop. Resilience is a complementary factor to directly countering threats by taking actions to backup information, having access to additional equipment as needed, by budgeting for failure, preparing for unexpected circumstances among other activities. Concepts from evolution and game theory are introduced within the resilience discussion.

INTRODUCTION

This article includes an approach to cyber security from the perspective of resilience. The World Economic Forum beta framework, a general systems model, and Ashby's Law of Requisite Variety are used as a lens to explore the topic. While the literature on resilience or cyber resilience is readily available and actionable from such organizations as the Department of Homeland Security, the connections among resilience frameworks, game theory, and evolutionary processes are limited. This short and nontechnical paper includes an organizational generic cyber security problem, the purpose of the paper, a few key definitions, some frameworks, analysis, future research, and conclusions. Objectives include providing an approach to cyber resilience and some reasons why cyber counter measures while necessary, are not sufficient.

DOI: 10.4018/978-1-5225-8897-9.ch057

BACKGROUND

Several definitions of resilience are listed, with each adding some helpful ideas about the topic.

- **Cyber or CYBER:** The National Security Agency or NSA (2018) defined "CYBER - a prefix used to describe a person, thing, or idea as part of the computer and information age. Cyber Warfare is defined as a war fighting discipline that integrates instruments of military power to achieve and sustain U.S. superiority in network communication through the integrated planning, execution, and assessment of offensive and defensive capabilities" (NSA, 2018).
- **Evolution:** Fichter, Pyle, and Whitmeyer (2010) noted "Evolutionary change is any process that leads to increases in complexity, diversity, order, and / or interconnectedness" (p. 58).
- **Resilience:** The concept is attributed to the ability to learn, self-organize, become financially stable, and adapt to disturbances in the environment (Sudmeier-Rieux, 2014). The Stockholm Resilience Centre (2018) noted, "resilience is the capacity of a system, be it an individual, a forest, a city, or an economy, to deal with change and continue to develop. It is about how humans and nature can use shocks and disturbances like a financial crisis or climate change to spur renewal and innovative thinking."
- **Resilience:** The Department of Homeland Security or DHS (2018) defined resilience as "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents." DHS includes examples of resilience measures as having a business continuity plan, using a generator for backup power, and using durable building materials.

The common element among these and other definitions of resilience is the notion, not of winning directly and outright, but of surviving, adapting, mitigating, and recovery—bouncing back in simple terms. Winning or losing are temporary situations unless the loss is sufficient to cause a system collapse. Typically, resilience is ongoing and something to evolve and improve over time.

The high-level organizational problem is the ongoing and escalating conflict between cyber security threats and the capability of organizations to effectively respond to them. Essentially, this situation is a conflict between two or more parties: an attacker and a defender where the defender may not know who or what to expect. Senge (2006) described this concept using the escalation archetype, which provides a visual image of conflict. Linkov, Eisenberg, Plourde, Seager, Allen, and Kott (2013) noted, while progress has been made with respect to cyber risks, "it is clear that anticipation and prevention of all possible attacks and malfunctions is not feasible." The (Presidential Policy Directive 21 2013) and the executive order (Executive Order 13636 2013) were released to address organizational cyber-infrastructure to counter cyber-attacks.

ORGANIZATIONAL RESILIENCE

Problems

There are the issues of frequency and costs, which include various perspectives and estimates but not always convergence, in addition to the issues of attacks and defense. Accenture (2017) noted, cyber-