Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 28 (2014) 838 – 847

Procedia Computer Science

Conference on Systems Engineering Research (CSER 2014)

Eds.: Azad M. Madni, University of Southern California; Barry Boehm, University of Southern California; Michael Sievers, Jet Propulsion Laboratory; Marilee Wheaton, The Aerospace Corporation
Redondo Beach, CA, March 21-22, 2014

Cyber Resiliency Engineering

Overview of the Architectural Assessment Process

Deborah J. Bodeau[a], Richard D. Graubart[b], and Ellen R. Laderman[c] *

a, b, c *The MITRE Corporation 202 Burlington Road Bedford MA 01730, USA*

Abstract

Missions, business functions, organizations, and nations are increasingly dependent on cyberspace where attacks are no longer limited to simple discrete events such as the spread of a virus or a denial-of-service attack. Therefore, architecture and systems engineering must assume systems or components have been compromised and missions and business functions must continue to operate despite compromises. A growing number of technologies and architectural practices can be used to improve resilience to cyber threats. However, these improvements come with costs as well as benefits. Cyber resiliency assessments are intended to identify where, how, and when cyber resiliency techniques can be applied to improve architectural resiliency in a cost-effective way.

Keywords: cyber resiliency engineering, cyber resiliency assessment, architectural assessment process

*Deborah J. Bodeau Tel.: 1-781-271-8436; fax: 1-781-271-8953; E-mail address: dbodeau@mitre.org
Richard D. Graubart Tel.: 1-781-271-7976; fax: 1-781-271-8953; E-mail address: rdg@mitre.org
Ellen R. Laderman Tel.: 1-781-271-4940; fax: 1-781-271-3957; E-mail address: laderman@mitre.org

doi:10.1016/j.procs.2014.03.100

1. Introduction

With the growing capability, expertise and intent of advanced cyber adversaries, it is no longer realistic to assume that one can successfully keep all adversaries out of a system infrastructure. Therefore, architecture and systems engineering must be based on the assumption that systems or components have been or can be compromised, and that missions and business functions must continue to operate in the presence of compromise [1]. Cyber resiliency assessments [2] are intended to identify where, how, and when cyber resiliency techniques can be applied to improve architectural resiliency against advanced cyber threats. The Cyber Resiliency Engineering Framework [3], as illustrated in Figure 1 and described in more detail in the Appendix, provides a way to understand goals and objectives based on this assumption of compromise, and the techniques (as defined in Table 5 below) that can be applied to improve mission resilience against advanced cyber threats.

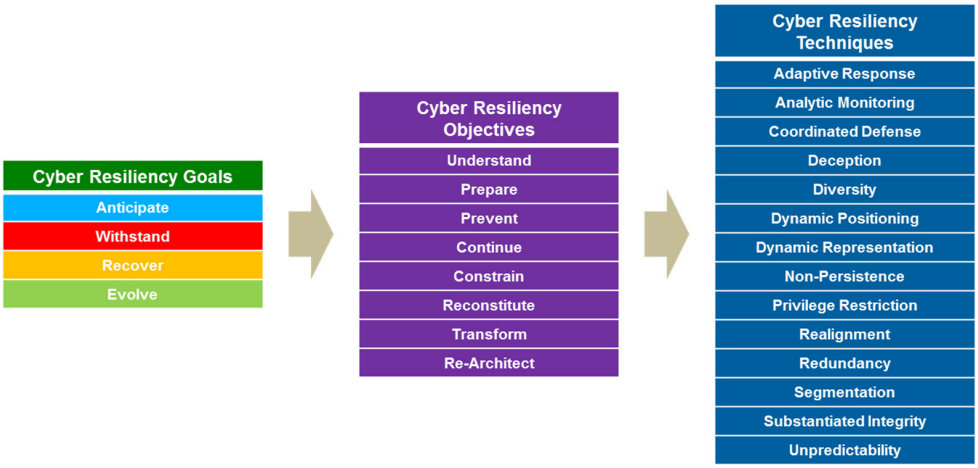

Figure 1. Cyber Resiliency Engineering Framework

However, due to a variety of political, operational, economic and technical (POET) factors, it is not feasible for organizations to use all resiliency techniques, or the growing set of technologies that implement aspects of the techniques. (For a detailed survey of technologies, as well as discussion of POET factors, see [2].) It is also not feasible to apply any resiliency technique pervasively, because implementations of cyber resiliency techniques vary in maturity across different architectural layers, and because some implementations are intended to be used only in strategically chosen locations in a system, common infrastructure, or System of Systems (SoS). Thus, a structured approach to identifying possible improvements is needed. The following three steps are used to assess the cyber resiliency of a system or architecture: (1) determine the scope of, and prepare for, the assessment, (2) assess the architecture, and (3) develop specific recommendations.

If the approach is applied to an operational or as-is architecture, the emphasis may be on “low-hanging fruit” or opportunities for near-term and high-leverage improvements, using a few cyber resiliency techniques. A set of general recommendations provides a starting point for identifying such opportunities. If the approach is applied to a notional or to-be architecture, the assessment may look at the full set of cyber resiliency techniques, and at ensuring that possible solutions in the mid- and long-term can be integrated into the architecture.

2. Determine the Scope and Plan for the Assessment

Planning an assessment involves determining the purpose and scope of an assessment and identifying key stakeholders and sources of information.

The purpose of an assessment is defined by the questions it is intended to answer and the decisions it is intended to support. These should initially be expressed in stakeholder terms rather than resiliency terms; they can then be