Architect to Protect:
Creating a Foundation for Resiliency

This paper outlines best practices for #1 Architect to Protect.

Planning and Preparation Activities	***Recovery and Reconstitution Activities***
0. Disrupting the Attack Surface	
*1. **Architect to Protect*** *2. Secure Administration* *3. Access Control* *4. Device Hardening* *5. Backup Strategies* *6. Cyber Continuity of Operations (COOP) Planning*	*7. Cyber COOP Execution* *8. Secure Communications* *9. Core Services* *10. Data Recovery Strategies* *11. Forensics* *12. After Action Activities*

The BIG Idea

By building resiliency protections into its cyber architecture, an entity or mission can create a foundation of resiliency that will ensure operational continuity and efficacy despite the efforts of advanced adversaries.

Cyber Resiliency Goals & Objectives

The Architect to Protect activity is most often used by an entity that has identified *Evolve*[1] and *Withstand* as a goal and *Transform*, *Re-Architect*, *Prepare*, *Continue*, and *Constrain* as objectives.

Design Principles

The design principles for architectural foundations enable resilience-enhancing technologies to be integrated with security and other infrastructure services in a cost effective way.

- *Segmentation*: Don't give the adversary freedom to move laterally; architect the network and shared services so that portions can be isolated.
- *Coordinated Defense*: Apply technical Defense-in-Depth effectively using multiple protections at multiple architectural layers; provide processes and tools to manage protections consistently; define business processes that enable cyber defenders to collaborate.
- *Diversity*: Capitalize on and manage diversity in enterprise systems and processes. Managed diversity reduces the effectiveness of attacks targeted at a particular system type by introducing multiple layers of friction in the cyber attack lifecycle.

What Can Be Done Now

The following resiliency techniques can help transform business processes and redesign systems to use existing technologies more effectively:

- *Segmentation*

[1] All italicized words are defined in the *Cyber Resiliency Terms and Concepts* document.

  - Predefine enterprise-internal enclaves based on criticality and sensitivity.
  - Isolate the enterprise security operations or response center from the rest of the enterprise.
  - Segment enterprise directory services (e.g., Active Directory or Apache Directory Server) on the basis of work roles and/or segment enterprise directory services into multiple enclaves based on criticality or sensitivity.
- *Coordinated Defense*
  - Implement layered boundary defenses at key points in the enterprise. This would include at the external perimeter (e.g., organizational firewalls), key application points (e.g., email and application servers) and client endpoint protection (e.g., user laptops, tablets and smartphones).
  - Define processes and employ tools to help system administrators and cyber defenders share information and collaborate; create a culture of shared situational awareness.
  - Perform a consistency analysis to ensure that roles and responsibilities, particularly with respect to COOP, are defined for synergy rather than conflict.
- *Diversity*
  - Identify sources of diversity (e.g., different versions of similar products acquired at different times or by different business units, BYOD).
  - Define a strategy for managing diverse implementations consistently and applying different approaches to diversity (e.g., Architectural Diversity, Design Diversity, Information Diversity, Command, Control And Communications Path Diversity, or Supply Chain Diversity).
  - Use multiple security products including Antivirus and Anti-Malware at multiple layers allowing for defensive diversity throughout the cyber attack lifecycle.

The Right People & Policies

Creating a foundation of resiliency requires specific skills and policies:

- An enterprise architect who understands the potential consequences of APT activities and destructive malware as well as cyber resiliency goals, objectives, and techniques
- System administrators and cyber defenders with a culture of collaboration, shared situational awareness and shared broad responsibility
- Governance structures that enable coordination of protection mechanisms should be socialized from the board level down through the lowest level of the organization
- Strategic planning to ensure that evolution of enterprise architecture results in more resilience opportunities, rather than in a larger and less knowable attack surface

Cyber Attack Lifecycle[2]

Using the cyber resiliency techniques, *segmentation*, *coordinated defense* and *diversity*, as described above, defenders can impede the adversary's attack on the enterprise and limit the damage the malware causes. The use of *segmentation* and *diversity* can negate or degrade the adversary's delivery of malware. When the adversary attempts to initiate the exploit, employ mechanisms to manage the initial victims, and execute the attack plan, the *coordinated defense* technique in concert with *diversity* and *segmentation* techniques impede these efforts and contain their effects.

[2] The Cyber Attack Lifecycle is described in the *Cyber Attack Lifecycle and Resilience* document.

Synergies & Barriers

The enterprise architecture must ensure that practices in other areas (such as Secure Administration, Access Control, Data Recovery Strategies, and Forensics) have not been rendered technically infeasible, ineffective, or costly.

Synergies among practice areas should be pursued, such as those between technical Defense-in-Depth and

- *Diversity*, by using multiple security products (e.g., multiple anti-virus products, anomaly detectors)
- *Coordinated Defense*, by defining processes to ensure that security protections applied at multiple architectural layers or locations are used consistently

Barriers to adoption include

- Cultural resistance to coordination among administrators, as well as among administrators and cyber defenders
- Life-cycle and security management costs, particularly for architectural and design Diversity

Just Ahead

The enterprise architecture should accommodate emerging technologies, such as those that enable dynamic segmentation and resource isolation, and those used in synthetic Diversity. It should also be able to accommodate new segmentation capabilities related to the Internet of Things, e.g., placing HVAC or lighting control services on a separate segment than business functions.