Disrupting the Attack Surface:
Making Life Hard for the Adversary

This paper outlines best practices for Disrupting the Attack Surface.

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

Whereas the other activities (1-12) focus on reducing the attack surface, the scope of this activity is on disrupting the attack surface. Changing the attack surface in such a way that the adversary is unable to get correct and timely information about the defenders, makes incorrect assumptions about the defenders, wastes resources or prematurely discloses malware to the defenders, and provides defenders an opportunity to get ahead of the attack and defeat the adversary.

Cyber Resiliency Goals & Objectives

The Disrupt the Attack Surface activity is most often used by an entity that has identified *Anticipate*[1]*, Withstand* and *Recover* as goals and *Understand, Prevent*, *Continue*, and *Constrain* as objectives.

Design Principles

The design principles for disrupting the attack surface create an uncertain environment for the adversary and thus make it more difficult for the adversary to effectively and successfully attack the enterprise.

- *Adaptive Response:* Optimize the organization's ability to respond in a timely and appropriate manner to adversary activities, thus maximizing the ability to maintain mission/business operations, limit consequences, and avoid destabilization.
- *Deception*: Mislead or confuse the adversary, or hide critical assets from the adversary, making them uncertain how to proceed, delaying the effect of their attack, increasing the risk to them of being discovered, causing them to misdirect or waste their attack, and expose their tradecraft (e.g., Attacker TTPs) prematurely.
- *Dynamic Positioning*: Impede an adversary's ability to locate, eliminate or corrupt mission/business assets, and cause the adversary to spend more time and effort to find the organization's critical assets, thereby increasing the chance of the adversary revealing their actions and tradecraft (e.g., Attacker TTPs) prematurely.
- *Non-Persistence*: Reduce exposure to corruption or modification; provide a means of curtailing an adversary's advance and potentially expunging an adversary's foothold from the system.

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

- *Realignment*: Reduce the attack surface of the defending organization by minimizing the chance that non-mission/business functions could be used as an attack vector.
- *Unpredictability:* Increase the adversary's uncertainty regarding the cyber defenses that they may encounter, thus making it more difficult for them to ascertain the appropriate course of action.

What Can Be Done Now

The following resiliency techniques can help transform an easily attacked enterprise into one that can better resist and recover from attacks:

- *Adaptive Response*
  - Reallocate resources to tasks or functions to manage risks without terminating functions or processes.
  - Change how defensive mechanisms are used based on changes in the operational environment as well as changes in the threat environment.
- *Deception*
  - Establish, maintain, and direct adversaries to deception environments causing adversaries to unintentionally divulge information about the nature of their attack in a safe setting.
  - Provide deliberately false information to mislead and possibly track adversaries.
- *Dynamic Positioning*
  - Physically or logically relocate assets and functionality making it harder for adversaryies to successfully target them, and increasing chances that adversary's actions will be detected.
  - Physically or logically relocate defensive mitigations (including sensors) making the defensive landscape more challenging for adversary's to traverse.
- *Non-Persistence*
  - Refresh services to eliminate adversary foothold.
  - Refresh connections to minimize adversary's ability to gain or extend foothold.
- *Realignment*
  - Offload supportive but non-essential functions to a service provider that is better able to support the functions.
  - Reduce the attack surface by removing, replacing or disabling risky implementations.
- *Unpredictability*
  - Change behavior or state at times or in ways that the adversary can't readily determine, thus increasing the likelihood that the adversary will misread the defensive landscape impeding the success of their planned activities.

The Right People & Policies

Increasing resiliency by reducing the attack surface 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 and shared situational awareness.
- Strategic planning to ensure that efforts to reduce the attack surface keep pace as the enterprise architecture evolves.

Cyber Attack Lifecycle[2]

Using the cyber resiliency techniques described above, enables the defenders to have a broad range of impacts on the adversary across the cyber attack lifecycle. In the early stages, the techniques impede the adversary, limit the knowledge the adversary can gain and sometimes even expose the adversary's actions. During the middle and later stages of the lifecycle, when the adversary is trying to deliver malware, exploit initial targets, take control of them and then execute and maintain control of the environment, the combination of resiliency techniques can detect the adversary's actions, limit the damage caused by these actions and redirect them to deception environments (e.g., honey nets) where the adversary's actions can be safely studied. In some cases a specific attack may even be precluded completely by these techniques.

Synergies & Barriers

The techniques discussed here have many synergies with each other. These include:

- *Adaptive Response's* use of *Unpredictability*, *Non-Persistence* and *Dynamic Positioning* to more effectively adapt to the adversary's actions.
- *Deception's* use of *Unpredictability* and *Dynamic Positioning* in deceiving the adversary.
- *Dynamic Positioning's* use of Unpredictability, *Non-Persistence* and *Adaptive Response* to most effectively position key resources to maintain functionality while disrupting the adversary's actions.

Barriers to adoption include:

- Conflict between techniques such as that between *Realignment and Adaptive Response* and that between *Unpredictability* and *Adaptive Response.*
- Cultural resistance to the concept that the adversary may be, and probably is, already present in the environment.
- Some organizations will face challenges with regard to banking regulations (e.g., Sarbanes Oxley) for some implementations of deception techniques (e.g., false accounts will show up on a SOX audit report, false financial information could lead to SEC issues). These challenges are addressed best, prior to implementation with the support of the full corporate team - legal, executive, as well as technical representatives.

Just Ahead

The threat landscape is evolving. The advent of the Internet of Things greatly increases the attack surface. This increases the need of the defender to disrupt the attack surface. The ability to adaptively respond to the adversary in a more dynamic and real time manner becomes more important. Similarly, the ability to more quickly off load or reconfigure resources (e.g., organizations applying their "own special sauce" to configuration of their resources) thus making it more difficult for the adversary to confidently target their attacks, becomes more imperative. As time goes on, organizations will need to modify their infrastructure architecture to create an innocuous path that makes attackers noisier and more visible.

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