Secure Communications:
Protecting Response and Recovery from Compromise

This paper outlines the best practices for #8 Secure Communications.

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

A secure response infrastructure requires secure communications in order to keep cyber adversaries from inserting themselves into response and recovery processes. Secure communications is essential for ensuring that critical information and commands are received and delivered to the appropriate parties. This will keep adversaries from undermining response effectiveness, learning more about your organization's systems and procedures, and further entangling themselves in your organizational systems and networks.

Cyber Resiliency Goals & Objectives

Secure Communications support the *Withstand*[1] and *Recover* goals and the *Continue*, *Constrain*, and *Reconstitute* objectives.

Design Principles

As the organization deals with an incident, the design principles for Secure Communications ensure that communications and supporting services (identification, authentication, and authorization; system and network administration) are available and trustworthy.

- *Segmentation*: Isolate the cybersecurity operations/response center from inbound access of the enterprise network as hostile activity may be occurring in that portion of the network. Where response-related communications flow over the same circuits as ordinary enterprise network traffic, use encryption (e.g., a virtual private network or VPN) to keep it logically separate.
- *Substantiated Integrity*: Employ data validation mechanisms, to validate the integrity of the data and the authenticity of the sender.
- *Redundancy*: Ensure that incident response staff have multiple communication paths. This will ensure communications even if the primary secure communications path is compromised or otherwise unavailable.

What Can Be Done Now

Adapt existing architectural elements (e.g., routers, firewalls, VPNs) and define procedures to protect against adversary activities during response and recovery.

- *Segmentation*

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

Approved for Public Release. Distribution Unlimited. Case Number 15-3300. ©2015 The MITRE Corporation. All Rights Reserved.

  - Logically isolate the communications for security critical enclaves from ordinary enterprise operations.
  - Protect and isolate communications related to incident response and recovery.
- *Substantiated Integrity*
  - Require the use of cryptography to validate the authenticity of the sender.
  - Use strong identification and authentication mechanisms to validate identity of senders and recipients of sensitive communications.
- *Redundancy*
  - Provide alternate or out-of-band communications methods for response staff.

The Right People & Policies

- Policies and supporting processes for acquiring and maintaining alternate secure communications.

Cyber Attack Lifecycle

Using the cyber resiliency techniques, *segmentation*, *substantiated integrity* and *redundancy*, as described above, defenders can impede the adversary's attack on the enterprise and limit the damage the malware causes. The use of *segmentation* with *redundancy* limits the adversary's ability to execute the attack plan and maintain a presence in the enterprise. Using *substantiated integrity* the defenders are able to detect the adversary and curtail the adversary's ability to control mechanisms to execute the attack plan, and maintain a presence.

Synergies and Barriers

Synergies among practices include *Redundancy's* use of *Substantiated Integrity*.

Barriers to adoption include the following:

- The cost of procuring, deploying and supporting alternate secure communications.
- The technical challenges of isolating a Cyber Security Operations Center (CSOC)/Cyber Security Incident Response Team (CSIRT)enclave and ensuring interoperability with secure communications.
- The cost of employing strong authentication mechanisms in support of the secure communications.

Just Ahead

Advanced adversaries will have already achieved a foothold in the organization's infrastructure. They will use this position and stealth to compromise the organization's communication during recovery. In response the organization needs to deceive the adversary using false communication paths, causing the adversary to prematurely reveal their presence and techniques. *Diversity* combined with *redundancy* will also be used, to provide secure communication paths that are independent of the original paths, and not subject to the same attacks. In addition there are new tools for substantiated integrity that indicate whether a man-in-the-middle or a code inject attack has occurred.

Approved for Public Release. Distribution Unlimited. Case Number 15-3300. ©2015 The MITRE Corporation. All Rights Reserved.