Crisis Cyber Decision Making

*The OODA “Loop”*

**Allen Forbes**  
President, Certico Corporation  
aforbes@certicoconsulting.com  
(480) 502-2258
Overview

• Attacker Methodology & Points of Detection

• OODA Loop
  – Observe
  – Orient
  – Decide
  – Act

• Critical Connections
Model of the incident hacking-process
(adapted from Hacking Exposed)

1) Footprinting
   identify area of operation, e.g., network-address ranges

2) Scanning
   identify computers, OSs, servers

3) Enumeration
   identify user accounts, file shares, make and type of servers

4) Gaining Access
   attempt unauthorized access

5) Escalating Privilege
   if only user-access, gain full control

6) Pilfering:
   search system for clear-text passwords, and trust-relationships

7) Covering Tracks
   hide tools, clear logs, and remove other evidence

8) Creating Back Doors
   ensure continued access
Boyd’s OODA “Loop”

Sketch

Orientation shapes observation, shapes decision, shapes action, and in turn is shaped by the feedback and other phenomena coming into our sensing or observing window.

Also note how the entire “loop” (not just orientation) is an ongoing many-sided implicit cross-referencing process of projection, empathy, correlation, and rejection.
Emphasizing implicit guidance accounts for organizational friction and maximizes available time. *Soccer game.*

Constant interaction guides the organization, ensures communications, and flows expectations.
Decisions are explicit. Make them when you need to align or re-orient the actions of your team.

Decision making and re-orientation take time.

Implicit guidance and controls influence the teams actions until they re-orient.
Questions

Allen Forbes
President, Certico Corporation
aforbes@certicoconsulting.com
(480) 502-2258