NETWORK SEGMENTATION WITH INTERLOCKING CONTROLS: ***TEACHING NEW DOGS OLD TRICKS***

AGENDA

- INTRODUCTION
- THE PROBLEM
- DEFINITIONS
- CRITICAL COMPONENTS
- HOW TO JUSTIFY
- HOW TO IMPLEMENT

Ron Dilley

CISO, Warner Bros. Entertainment Inc.

Security Practitioner (20+ Years)

Programmer

Problem and Puzzle Solver

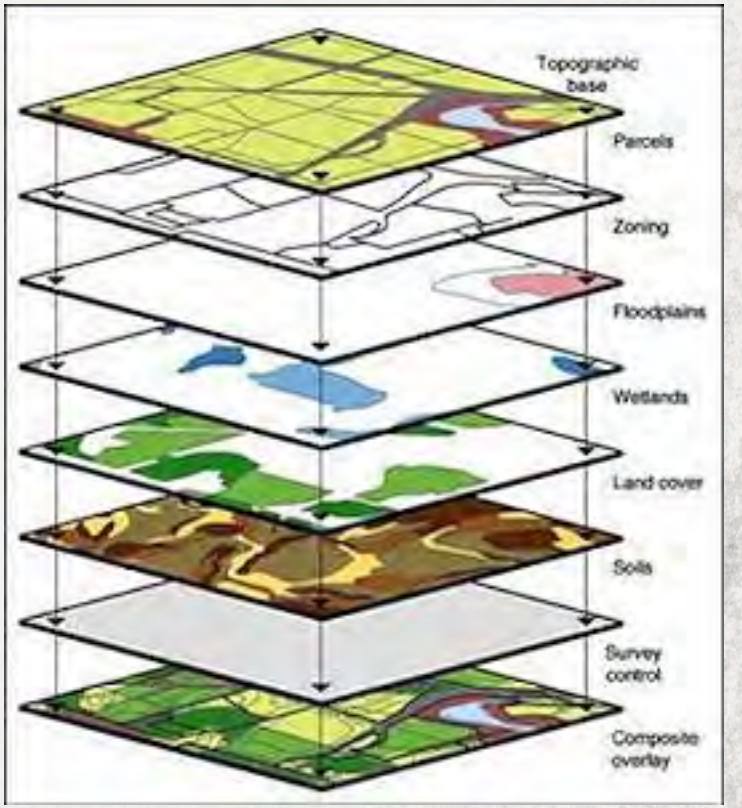
Security Curmudgeon (in training)

THE PROBLEM (AND A STORY)

vs.

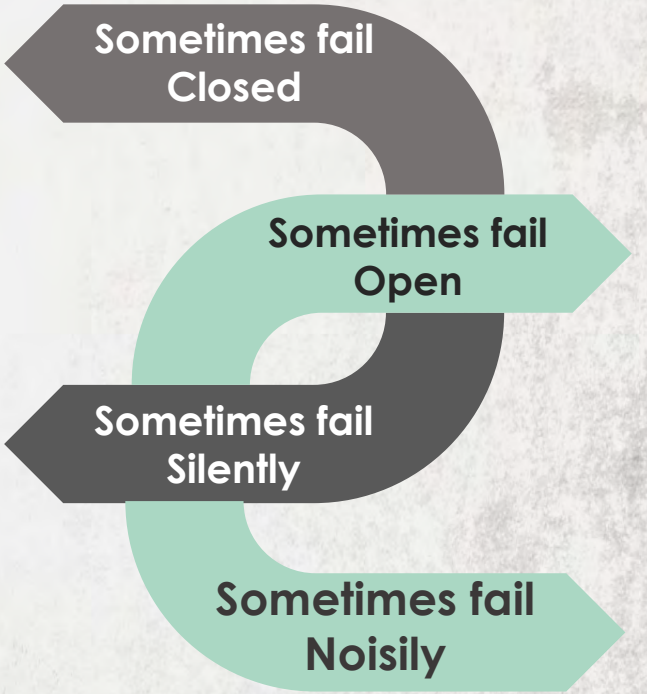
WHAT IS NETWORK SEGMENTATION

- One of the most important policy-centric controls you can have
- May be virtual (VLAN or addressing) or management (defined zones)
- A topological map, or a roadmap, are both management overlays atop a common data set
- Can you overlay your network or is it just an incomprehensible mess?



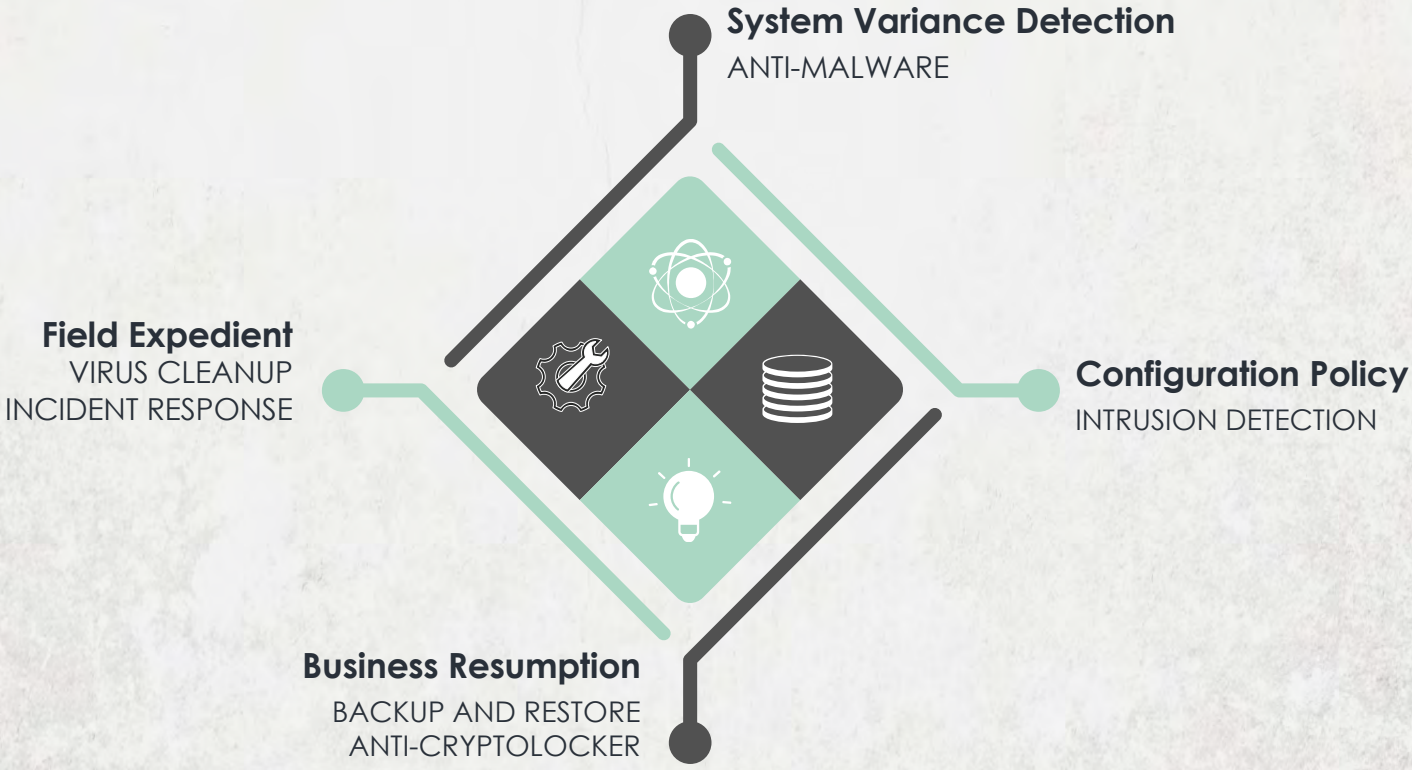
WHAT ARE INTERLOCKING CONTROLS: THE DOCTRINE (MARCUS RANUM/RON DILLEY)

- Each control should broadly influence a class of systems
- Each control should be configured to detect flaws or policy violations in others
- Each control should fail correctly by design
- Each control partially overlaps another



WHAT ARE INTERLOCKING CONTROLS: EXAMPLE

- Your configuration management is a primary capability for system configuration
- Your configuration management is a secondary capability for:

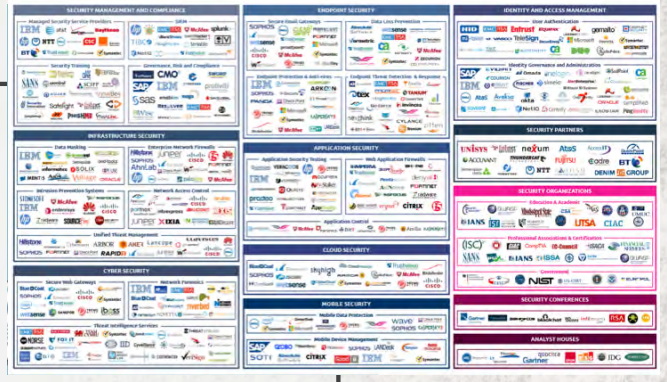


DEFENSE IN DEPTH VS. INTERLOCKING CONTROLS

Defense-in-depth

Back in the day

When I Started



Today

Interlocking Controls

- Broad influence (not a point solution)
- Improves the effectiveness of other controls
- Monitors for the effectiveness of other controls
- Can be implemented incrementally

CRITICAL COMPONENTS: SEGMENTATION AS AN ORGANIZER

- If you can define segments, then you can query your logs in terms like:

> **Tell me about engineering systems that are logging into the data center as "Administrator"**

> **Tell me about guest network systems that are attempting to log into the CFO's system cluster**

> **Tell me about administrative logins that are not originating from our privileged access management system**

CRITICAL COMPONENTS: EIGHT-LEGGED PLATFORM

- Runtime control
- Desktop configuration doctrines
- Configuration management
- Log collection, analysis and management
- File share/attachment management
- Segmentation
- Privilege management
- Policy violation detection

CRITICAL COMPONENTS: FAULT-DETECTING CONTROLS

- The first control may produce lots of alerts (save them but don't try to read them all!)
- The second control is configured to identify policy failures in the first (these are red alerts)

CRITICAL COMPONENTS: METRICS

- This is the only way you can understand what is happening
- If you don't have a way of measuring outcomes, any time you change anything, you can only *guess* as to its effect
  - You want to be able to make meaningful statements about the outcomes resulting from security interventions

HOW TO JUSTIFY

- Your plan will enable a secure and agile business, not limit it
- Your initiative will quickly enhance your defensible environment
- While strategically sustaining that posture as the threat-scape shifts
- It promotes a security aware culture
- It will progress incrementally on prioritized delivery
- It applies interlocking controls (not defense in depth)
- Your plan includes continual measurement and reporting as a foundational attribute

HOW TO IMPLEMENT

- A topic all to itself and we are almost out of time
- Start small (segment InfoSec then high value targets)
- Leverage incremental enhancements
- Response to security threats dovetail logically into this framework

Q&A