
black hat
USA 2016
Using an
EXPANDED
Cyber Kill Chain Model
to Increase Attack
Resiliency
Sean T Malone
@SeanTMalone
www.seantmalone.com
FusionX
www.FusionX.com
JULY 30 - AUGUST 4, 2016 / MANDALAY BAY / LAS VEGAS

Presenter Background

- 10+ Years in Offensive Information Security
- 4 Years of Adversary Simulation with FusionX
- Executing Realistic Attack Simulations – and Responding When it's NOT a Drill

Agenda

- Legacy Cyber Kill Chain Model
- The **Expanded** Cyber Kill Chain Model
  - The Internal Kill Chain
  - The Target Manipulation Kill Chain
- Understanding the Stages of a Sophisticated Attack
- Using the Expanded Model to Build a Resilient Enterprise

Legacy Cyber Kill Chain Model

Reconnaissance	• Harvesting email addresses, conference information, etc.
Weaponization	• Coupling exploit with backdoor into deliverable payload
Delivery	• Delivering weaponized bundle to the victim via email, web, USB, etc.
Exploitation	• Exploiting a vulnerability to execute code on victim's system
Installation	• Installing malware on the asset
Command & Control (C2)	• Command channel for remote manipulation of victim
Actions on Objectives	• With "Hands on Keyboard" access, intruders accomplish their original goal

From http://cyber.lockheedmartin.com/solutions/cyber-kill-chain

Legacy Cyber Kill Chain Model

"The Cyber Kill Chain model, as sexy as it is, reinforces old-school, perimeter-focused, malware-prevention thinking."

- Giora Engel, *Deconstructing The Cyber Kill Chain*, Dark Reading 2014

"Excellent for [external] attacks, but doesn't exactly work for insider threats."

- Patrick Reidy, *Combating the Insider Threat at the FBI*, Black Hat USA 2013

"In today's environment, every cyber attacker is a potential insider."

- Matt Devost, *Every Cyber Attacker is an Insider*, OODA Loop 2015

Legacy Cyber Kill Chain Model

"Perimeter Breach Kill Chain"

Reconnaissance	• Harvesting email addresses, conference information, etc.
Weaponization	• Coupling exploit with backdoor into deliverable payload
Delivery	• Delivering weaponized bundle to the victim via email, web, USB, etc.
Exploitation	• Exploiting a vulnerability to execute code on victim's system
Installation	• Installing malware on the asset
Command & Control (C2)	• Command channel for remote manipulation of victim
Actions on Objectives	• With "Hands on Keyboard" access, intruders accomplish their original goal

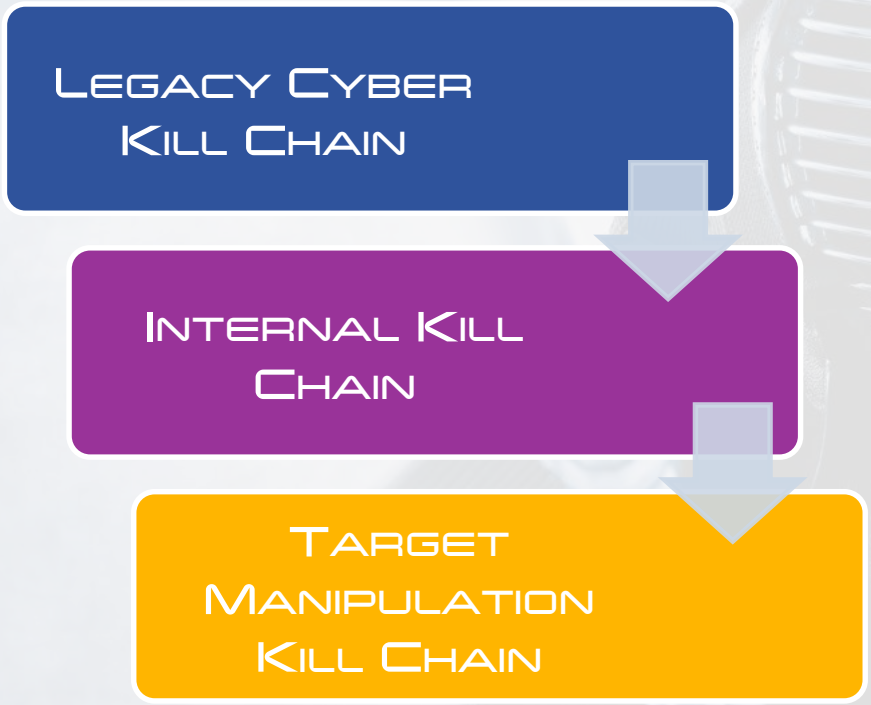
GAME OVER ?

What's an Objective?

Example Target Manipulation Objectives:

- Financial Theft
  - Modify queued wire transfers to redirect payments
- Reputation Impact and Loss of Market Share through DoS
  - Disable all company workstations
- Disable Infrastructure in Preparation for Kinetic Attack
  - Quickly cycle smart electric meters to overload grid
- Provide Propaganda Support for Coup Attempt
  - Hijack television broadcast
- Cause Terror in Regional Population
  - Change concentration of chemicals added to water supply

The EXPANDED Cyber Kill Chain Model

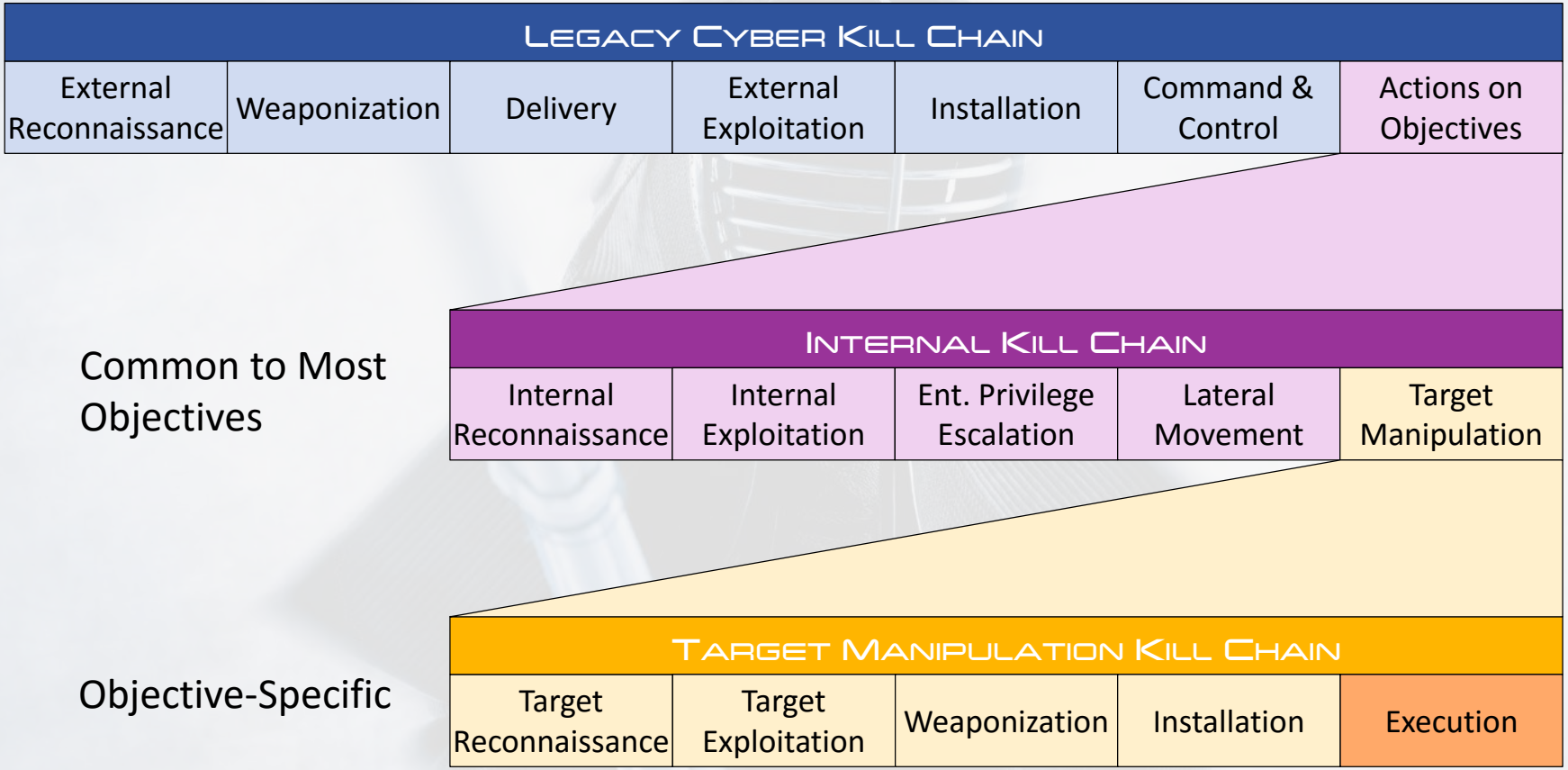


Breach the Enterprise Network Perimeter

Gain Access to Target Systems

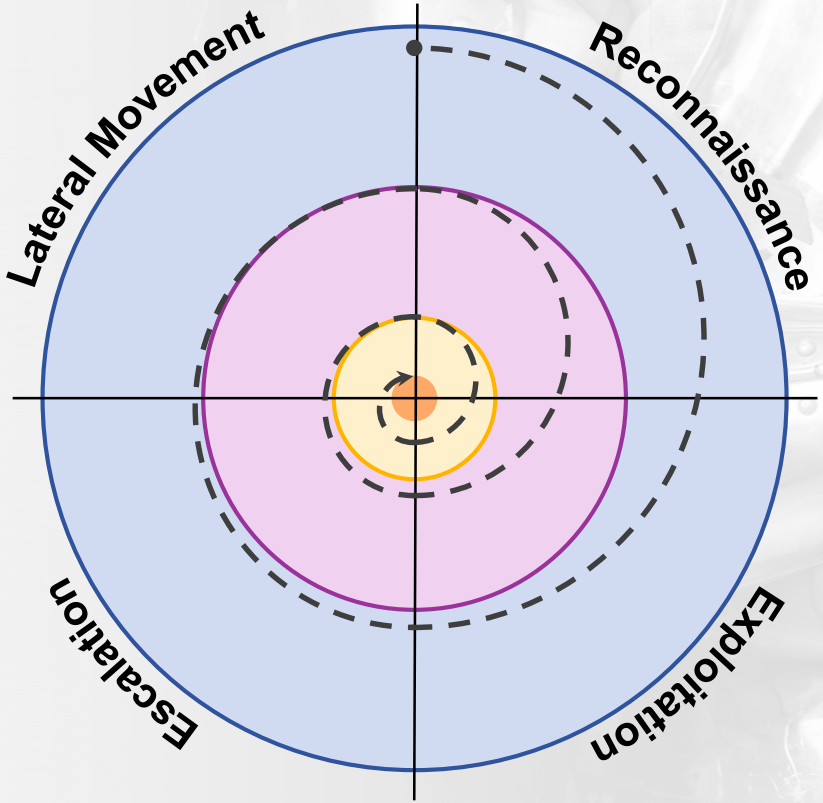
Manipulate Target Systems to Achieve Objective

The EXPANDED Cyber Kill Chain Model

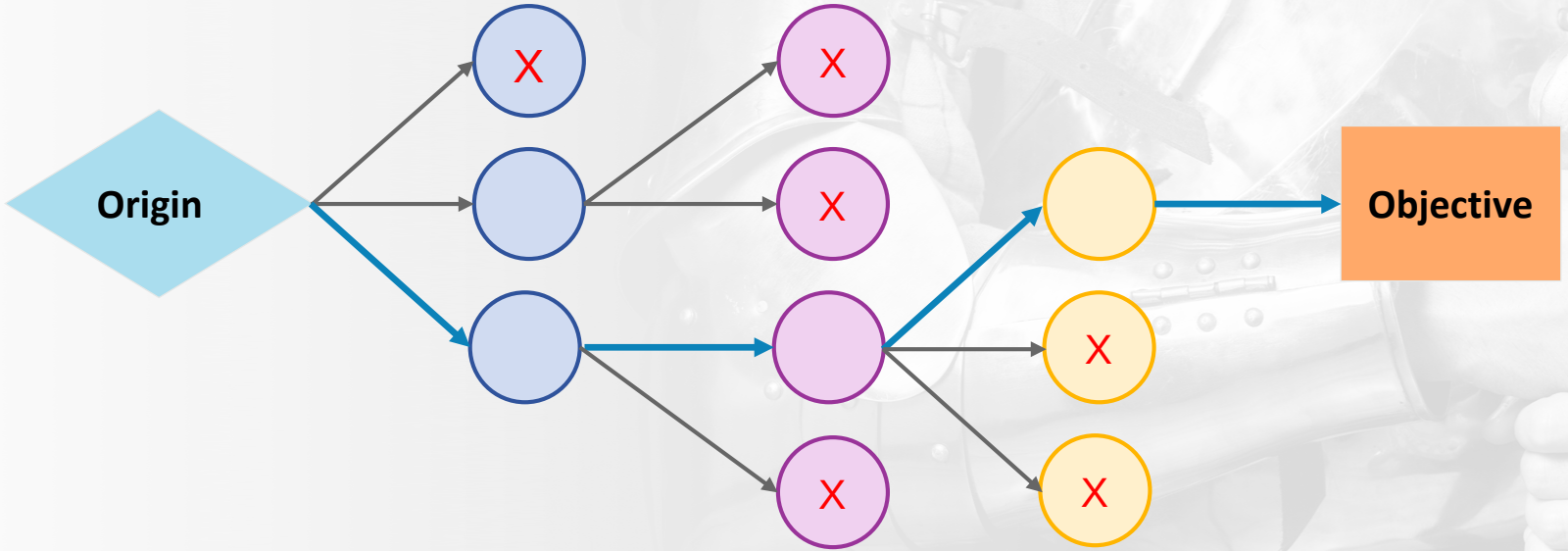


Kill Chain – Or OODA Loop?

Alternative: Spiral Model

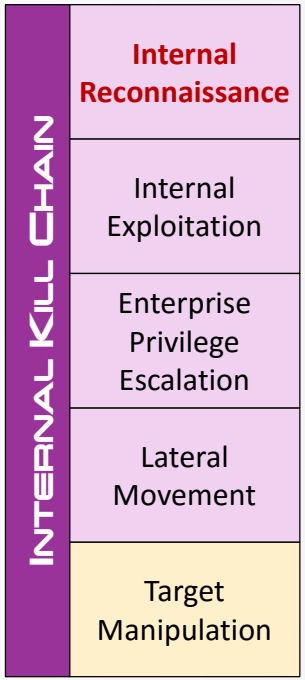


Alternative: Tree Model



Understanding the Stages of a Sophisticated Attack

Internal Reconnaissance



Objective

Data mine available systems and map the internal network and vulnerabilities

Time Required

1 to 2+ Weeks

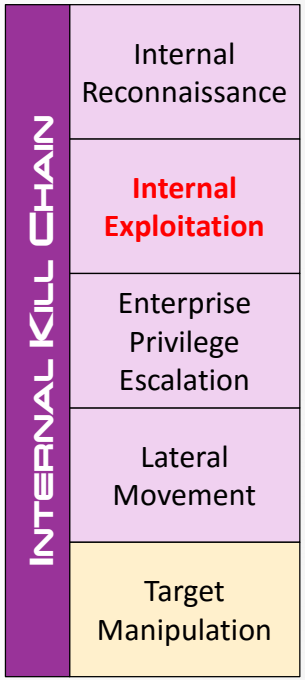
Offensive TTPs

- DOMEX of local files, network shares, browser history, wiki/SharePoint
- Light service probing

Defensive TTPs

- **Prevent**: Granular resource authorization
- **Detect**: Behavioral changes from this IP & user account

Internal Exploitation



Objective

Exploit information and vulnerabilities on internal systems

Time Required

2 Days

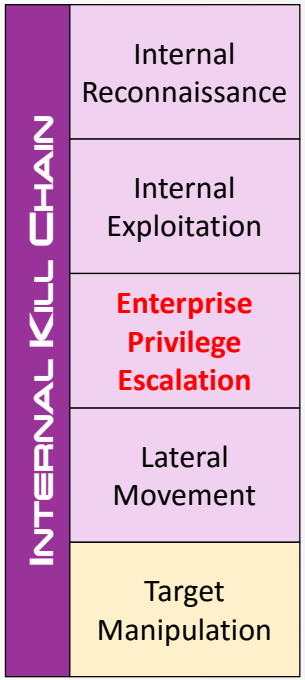
Offensive TTPs

- System vulnerabilities
- Web application vulnerabilities
- LLMNR/NBNS Spoofing

Defensive TTPs

- **Prevent**: Patch & vuln. management (including dev & test systems)
- **Detect**: Endpoint protection

Enterprise Privilege Escalation



Objective

Leverage compromised accounts and trust relationships to gain a high level of privilege

Time Required

1 to 3 Days

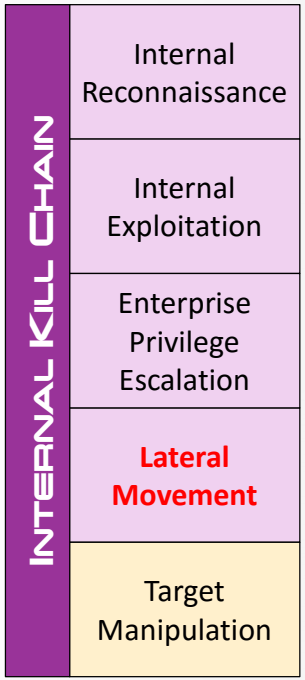
Offensive TTPs

- Kernel / system vulns.
- Pass-the-hash & Mimikatz
- Unprotected SSH keys
- Creds in configuration files

Defensive TTPs

- **Prevent**: Run as least-privilege accounts; use good security hygiene
- **Detect**: Behavioral analytics

Lateral Movement



Objective

Pivot through compromised systems into restricted network zones

Time Required

4 Hours

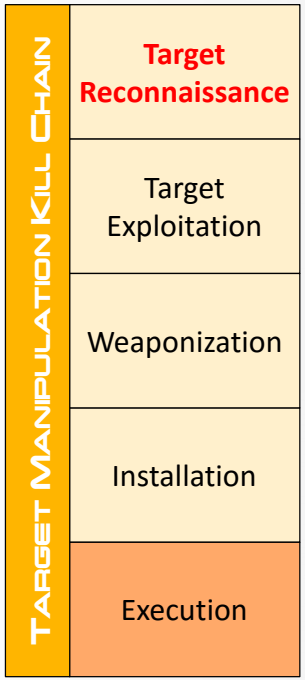
Offensive TTPs

- Target virtualization, backup, config management layers
- Layer SSH proxy tunnels to go deep

Defensive TTPs

- **Prevent**: Segmented security zones at all layers
- **Detect**: Behavioral analysis of successful login events

Target Reconnaissance



Objective

Map & understand objective-specific systems

Time Required

1 Week to 3 Months

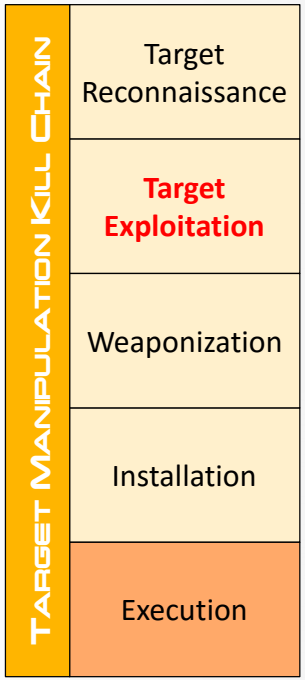
Offensive TTPs

- DOMEX of Vendor documentation, internal training, source code
- Standard admin utilities

Defensive TTPs

- **Prevent**: Restricted access to documentation & specifications
- **Detect**: Access patterns

Target Exploitation



Objective

Gain access to target systems via trust relationships or new vulnerabilities

Time Required

1 Hour

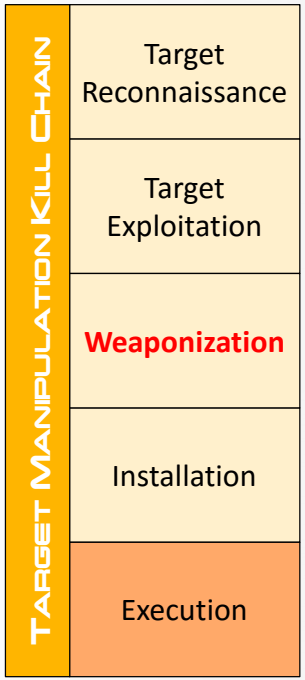
Offensive TTPs

- Default credentials, EOL systems, vendor backdoors
- Trust relationships with central authentication system

Defensive TTPs

- **Prevent**: Change defaults & segregate authentication
- **Detect**: Endpoint protection and behavioral analytics

Weaponization



Objective

Develop platform-specific malware to subvert target systems & business processes

Time Required

1 Week to 3 Months

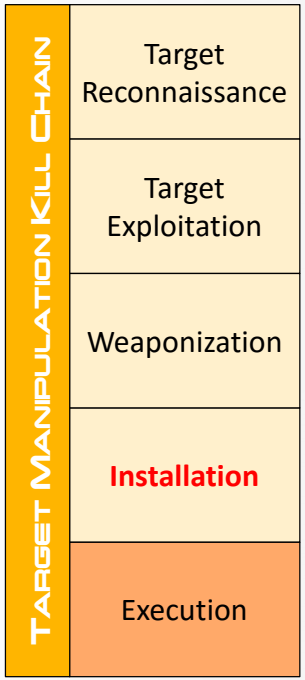
Offensive TTPs

- Duplicate target environment in a lab
- Extract, decompile, and reverse proprietary software

Defensive TTPs

- **Prevent**: Harden/obfuscate applications to make reversing difficult
- **Detect**: N/A - working offline

Installation



Objective

Deploy custom malware to target systems

Time Required

1 Hour

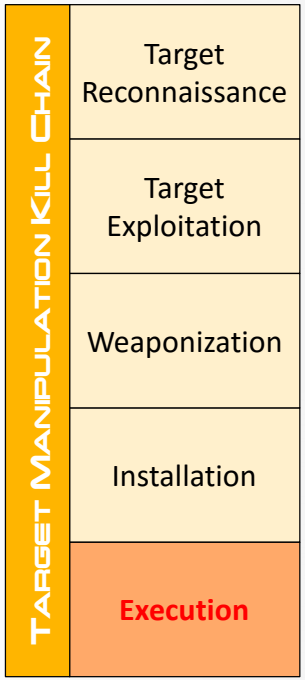
Offensive TTPs

- Patch or replace scripts, binaries, and configurations
- Tamper with detective controls

Defensive TTPs

- **Prevent**: Application signing
- **Detect**: File integrity monitoring, redundant processing systems

Execution



Objective

Activate malware to subvert target system operation, with material consequences

Time Required

1 Second

Offensive TTPs

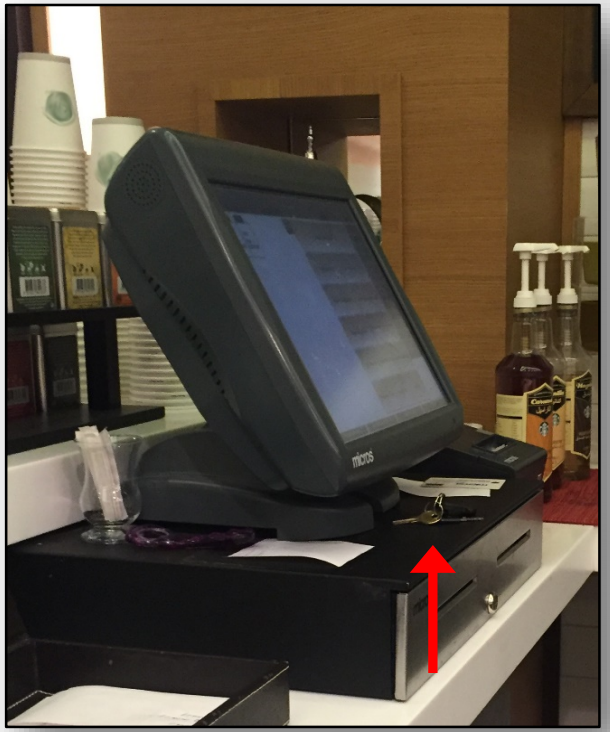
- Wait for optimal timing (market or geopolitical)
- May be all at once or slow damage over time

Defensive TTPs

- Response controls – have you war-gamed this?
- Breach insurance may help mitigate impact

Building a Resilient Enterprise

The Resilient Mindset



Every Control Will Fail

If the adversary has access to:

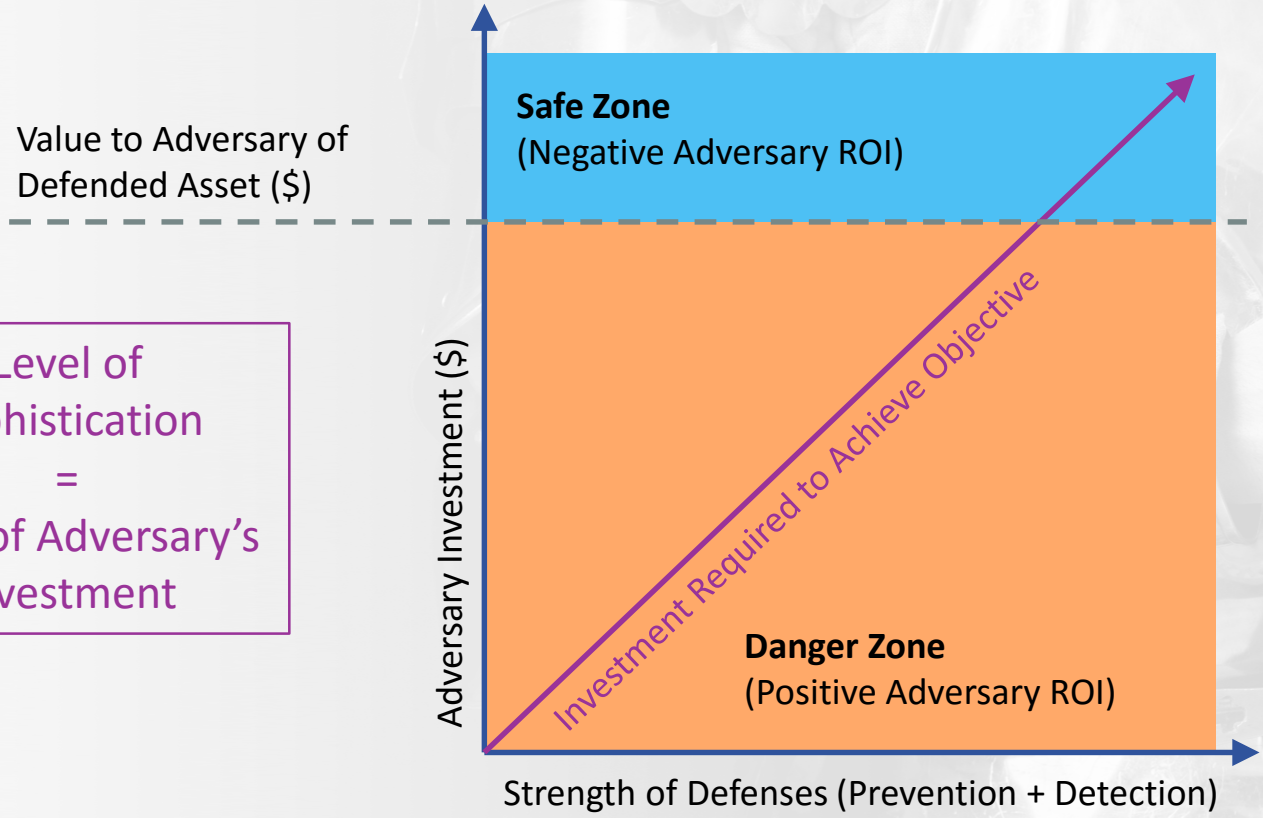
- The internal corporate network
- Any username and password
- All documentation & specifications

What would you do differently?

The Cyber Defense Threshold

Changing the Economics

Level of Sophistication = Level of Adversary's Investment



Final Thoughts, Questions, and Discussion

Sean T Malone
@SeanTMalone

(slides available at) www.seantmalone.com