BOW TIE MODEL OF DESTRUCTIVE MALWARE

ICS HISTORIAN CASE STUDY

INTRODUCTIONS

LUBOS MLCOCH

+ Customer Success – Cybersecurity Team
+ ~8 years with OSIsoft
+ Before: Senior Escalation Engineer

DANIEL MICHAUD-SOUCY

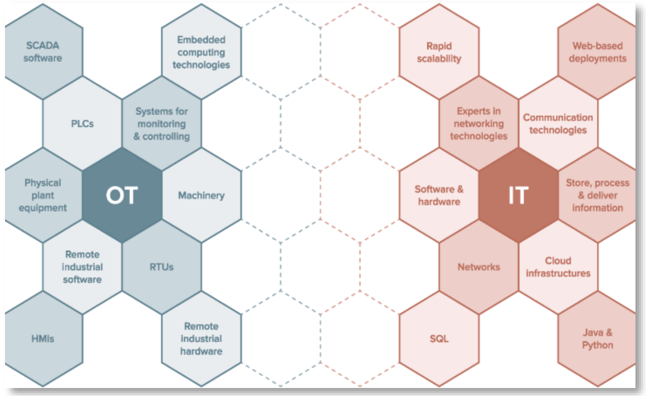
+ Industrial Pentester
+ ~3 years with Dragos
+ Before: Sempra Energy / SDG&E

SETTING THE STAGE

- ✓ THREATS TO ICS ENVIRONMENTS CONTINUE TO EVOLVE AND INCREASE
- ✓ UNDERSTANDING YOUR RISK POSTURE IS CRITICAL
- ✓ HOW TO EFFECTIVELY LEVERAGE THE BOW TIE MODEL
- ✓ COMMUNITY CONTRIBUTION OPPORTUNITIES

USE CASE

WHY DID WE DO THIS?



IT / OT
CYBERSECURITY GAP

DIGITAL
TRANSFORMATION

ENTERPRISE ACCESS
TO ICS DATA

USE CASE – RANSOMWARE

RAPIDLY EMERGING AS THE MOST VISIBLE CYBERSECURITY RISK.

LOTS OF LESSONS LEARNED FROM RECENT INCIDENTS.

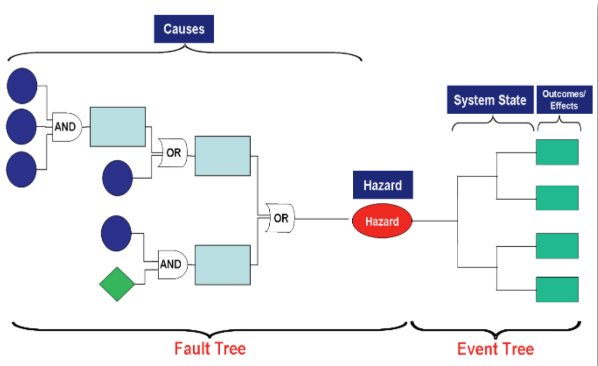
THE BOW TIE MODEL

RISK ANALYSIS AND MODELING

BOW TIE HISTORY AND OVERVIEW

BORN OUT OF A CATASTROPHE

Following the Piper Alpha incident of 1988, Shell Group adopted the Bow Tie model for risk analysis and modeling.



COMBINED METHODS OF RISK ANALYSIS

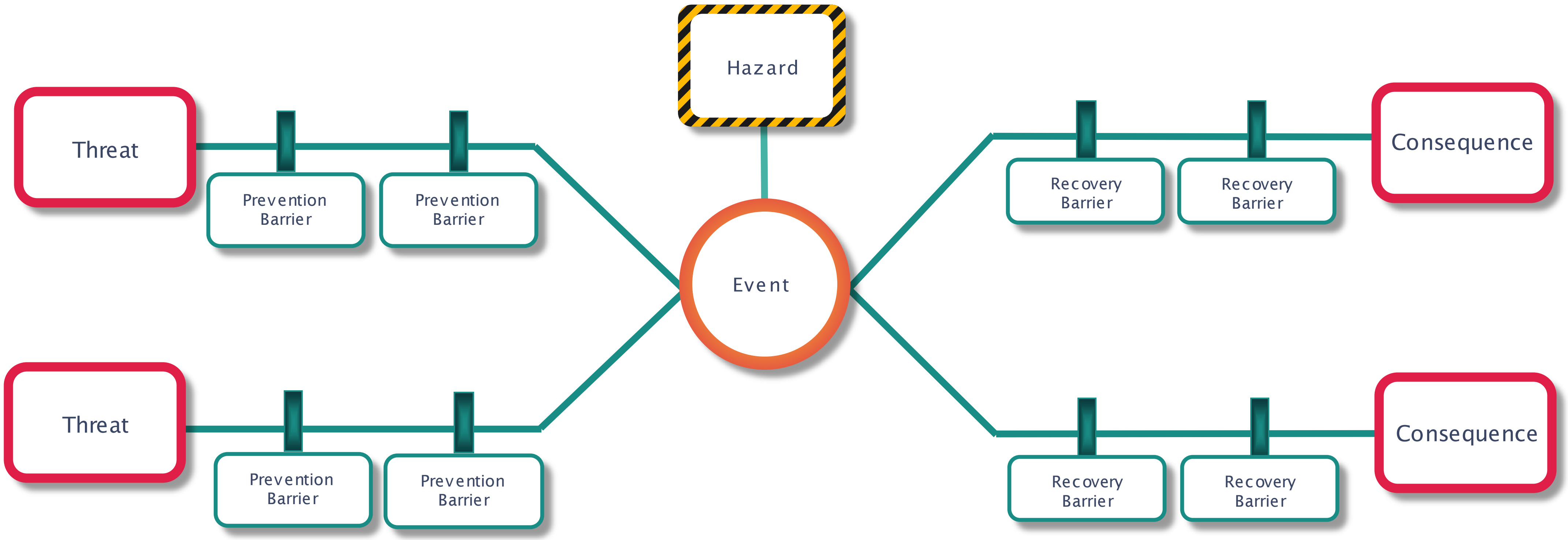
- Fault Tree Analysis
- Event Tree Analysis
- Causal Factors Charting

CONTROL IDENTIFICATION

Facilitates identification of the controls an organization has in place to prevent an event.

THE BOW TIE – AT A GLANCE

COMPONENTS AND DESIGN



ANATOMY

THE KNOT

HAZARD

THE HAZARD

Something that has the potential to cause damage. If control over the hazard is lost, this could lead to a negative impact. For example:

- Working with chemicals
- High voltages
- Fast moving machines

EVENT

THE EVENT

What happens when control over the hazard is lost. The negative impact is imminent. For example:

- Losing control over a vehicle
- Uncontrolled decompression
- Explosive material ignition

ANATOMY

THE LEFT SIDE

THREAT

THE THREATS

Whatever has the potential to cause your event. For example:

- Tire blowout
- Valve stuck close
- Brake failure

PREVENTION BARRIER

THE PREVENTION BARRIERS

Interrupt the scenario so the threats leading to the event are neutralized. For example:

- Anti-lock braking system
- Rupture discs
- PPE

ANATOMY

THE RIGHT SIDE

CONSEQUENCE

THE CONSEQUENCES

The potential outcome if the event is to occur. For example:

- Chemical spill
- Passenger expulsion from car
- Loss of power

RECOVERY BARRIER

THE RECOVERY BARRIERS

Limit the escalation of the scenario into actual impacts or mitigate the impact. For example:

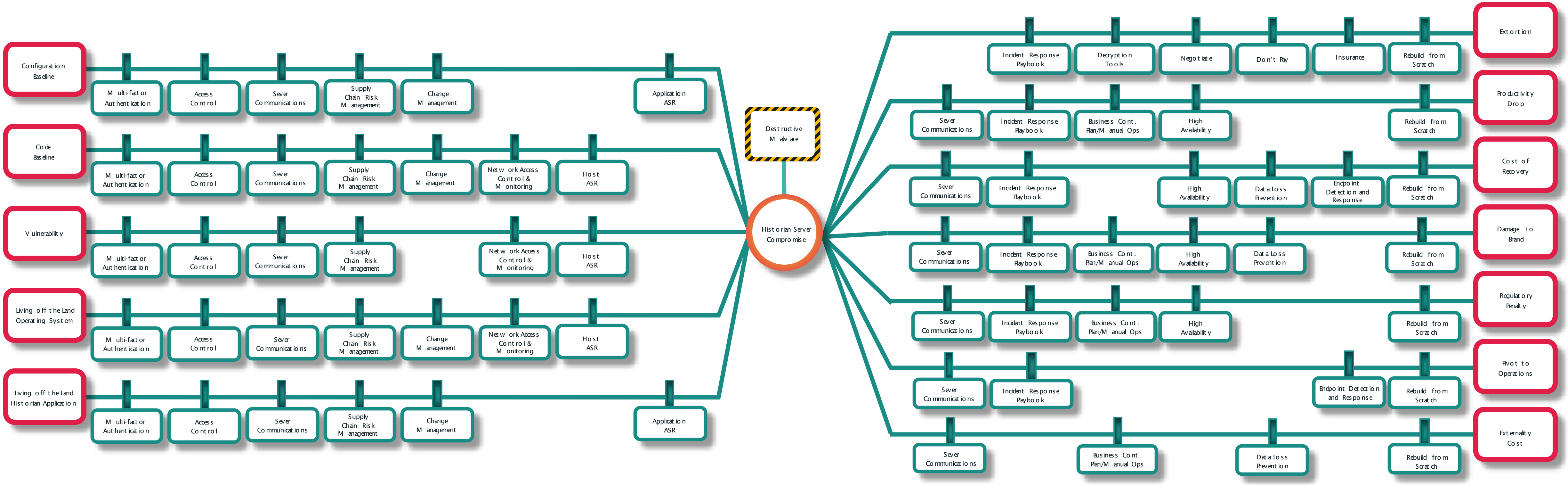
- Fire suppression system
- Seatbelt
- Backup power source

CASE STUDY: DESTRUCTIVE MALWARE ON ICS HISTORIAN

METHODOLOGY OVERVIEW

COLLABORATION AND RAPID IDEATION

- 3-month joint effort between OSIsoft and Dragos
- Informed by actual incidents (and near misses) of historian servers compromised by destructive malware
- Related experiences from subject matter experts

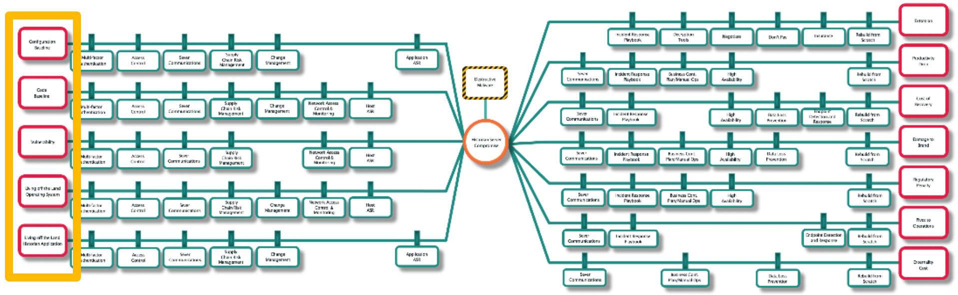


Configuration Baseline
Multi-factor Authentication
Access Control
Sever Communications
Supply Chain Risk Management
Change Management
Application ASR
Code Baseline
Multi-factor Authentication
Access Control
Sever Communications
Supply Chain Risk Management
Change Management
Network Access Control & Monitoring
Host ASR
Vulnerability
Multi-factor Authentication
Access Control
Sever Communications
Supply Chain Risk Management
Network Access Control & Monitoring
Host ASR
Living off the Land Operating System
Multi-factor Authentication
Access Control
Sever Communications
Supply Chain Risk Management
Change Management
Network Access Control & Monitoring
Host ASR
Living off the Land Historian Application
Multi-factor Authentication
Access Control
Sever Communications
Supply Chain Risk Management
Change Management
Application ASR
Destructive Malware
Historian Server Compromise
Incident Response Playbook
Decryption Tools
Negotiate
Don't Pay
Insurance
Rebuild from Scratch
Extortion
Sever Communications
Incident Response Playbook
Business Cont. Plan/Manual Ops
High Availability
Rebuild from Scratch
Productivity Drop
Sever Communications
Incident Response Playbook
High Availability
Data Loss Prevention
Endpoint Detection and Response
Rebuild from Scratch
Cost of Recovery
Sever Communications
Incident Response Playbook
Business Cont. Plan/Manual Ops
High Availability
Data Loss Prevention
Rebuild from Scratch
Damage to Brand
Sever Communications
Incident Response Playbook
Business Cont. Plan/Manual Ops
High Availability
Rebuild from Scratch
Regulatory Penalty
Sever Communications
Incident Response Playbook
Endpoint Detection and Response
Rebuild from Scratch
Pivot to Operations
Sever Communications
Business Cont. Plan/Manual Ops
Data Loss Prevention
Rebuild from Scratch
Externality Cost

METHODOLOGY OVERVIEW – THREATS

INSPIRATION AND FOUNDATIONAL CONCEPTS

- Inspired by the Electric Research Power Institute (EPRI) & Technology Assessment Methodology (TAM)



Configuration Baseline

Code Baseline

Vulnerability

Living off the Land Operating System

Living off the Land Historian Application

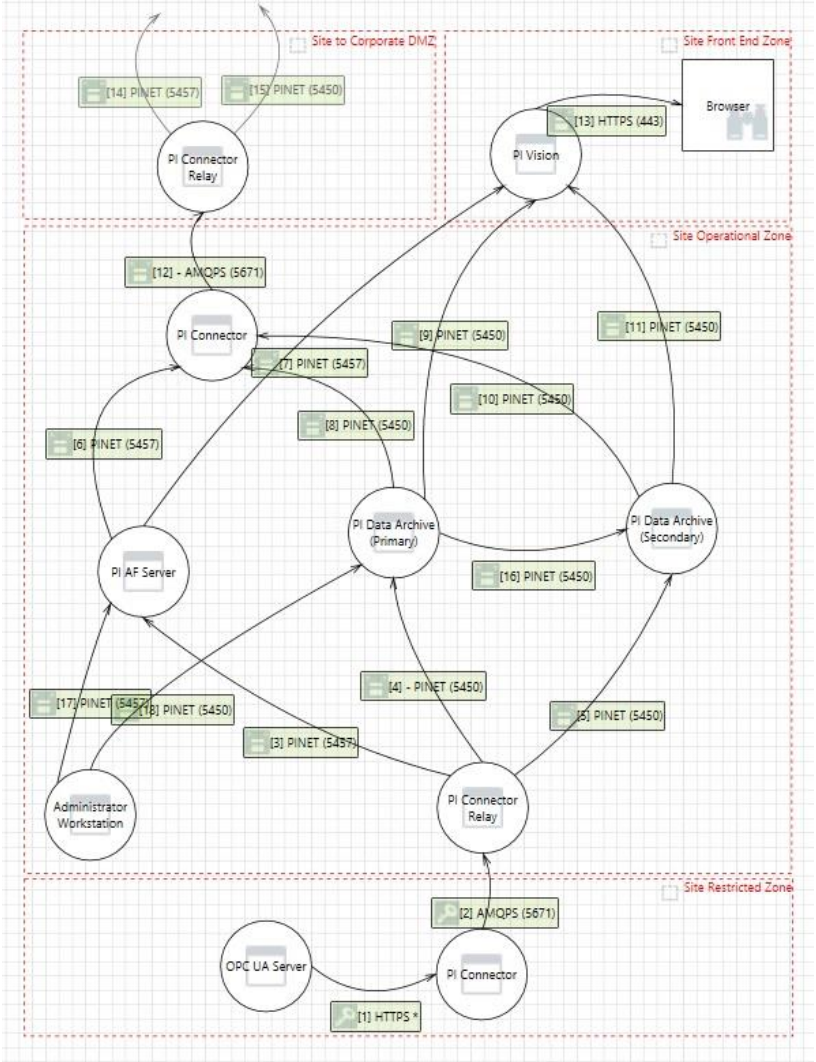
EPRI TECHNOLOGY ASSESSMENT METHODOLOGY

SYNERGY BETWEEN EPRI TAM AND BOW TIE MODELS

EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Cyber Security Technical Assessment Methodology

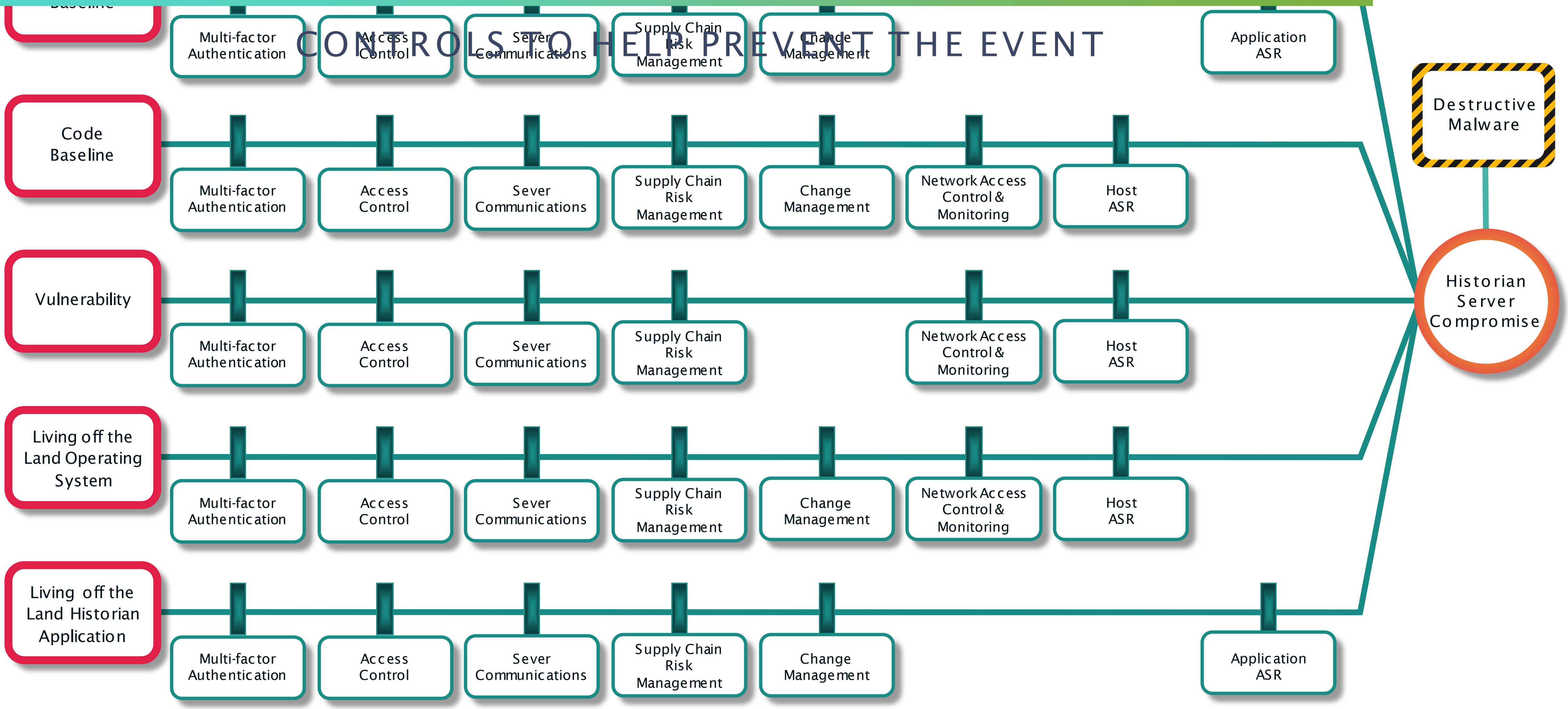
Risk Informed Exploit Sequence Identification and Mitigation, Revision 1



OSIsoft. DRAGOS

PREVENTION BARRIERS

CONTROLS TO HELP PREVENT THE EVENT



OSIsoft. DRAGOS

DEEP DIVE INTO A PREVENTION BARRIER

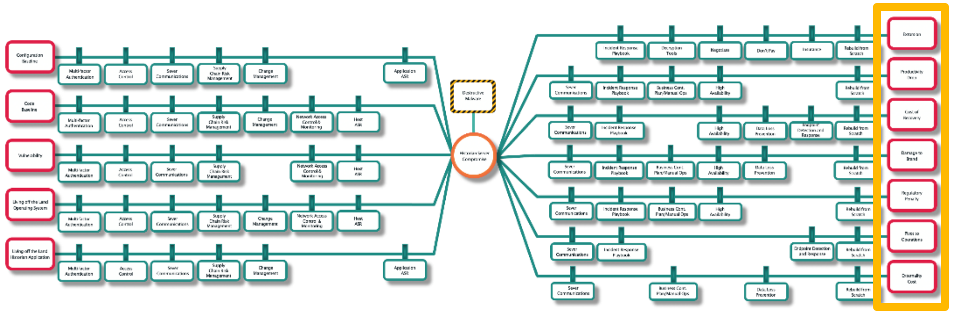
Security Effectiveness Score + Implementation Burden = Method Efficacy

Host ASR	Security Effectiveness Score			Implementation Burden		Method Efficacy		
	Protect	Detect	R/R	Initial	O&M	Protect	Detect	R/R
Server Core	High	None	Low	Medium	Medium	4/5	N/A	3/5
Application Whitelisting	High	Medium	None	High	High	3/5	2/5	N/A
Communications Whitelisting	Medium	Medium	None	High	High	4/5	3/5	N/A
User Access Control	Low	Low	None	Low	Low	4/5	4/5	N/A
Credential Guard	Medium	Medium	None	Low	Low	5/5	4/5	N/A

METHODOLOGY OVERVIEW – CONSEQUENCES

INSPIRATION AND FOUNDATIONAL CONCEPTS

- Informed by the Factor Analysis of Information Risk (FAIR) loss model categories



Extortion

Productivity Drop

Cost of Recovery

Damage to Brand

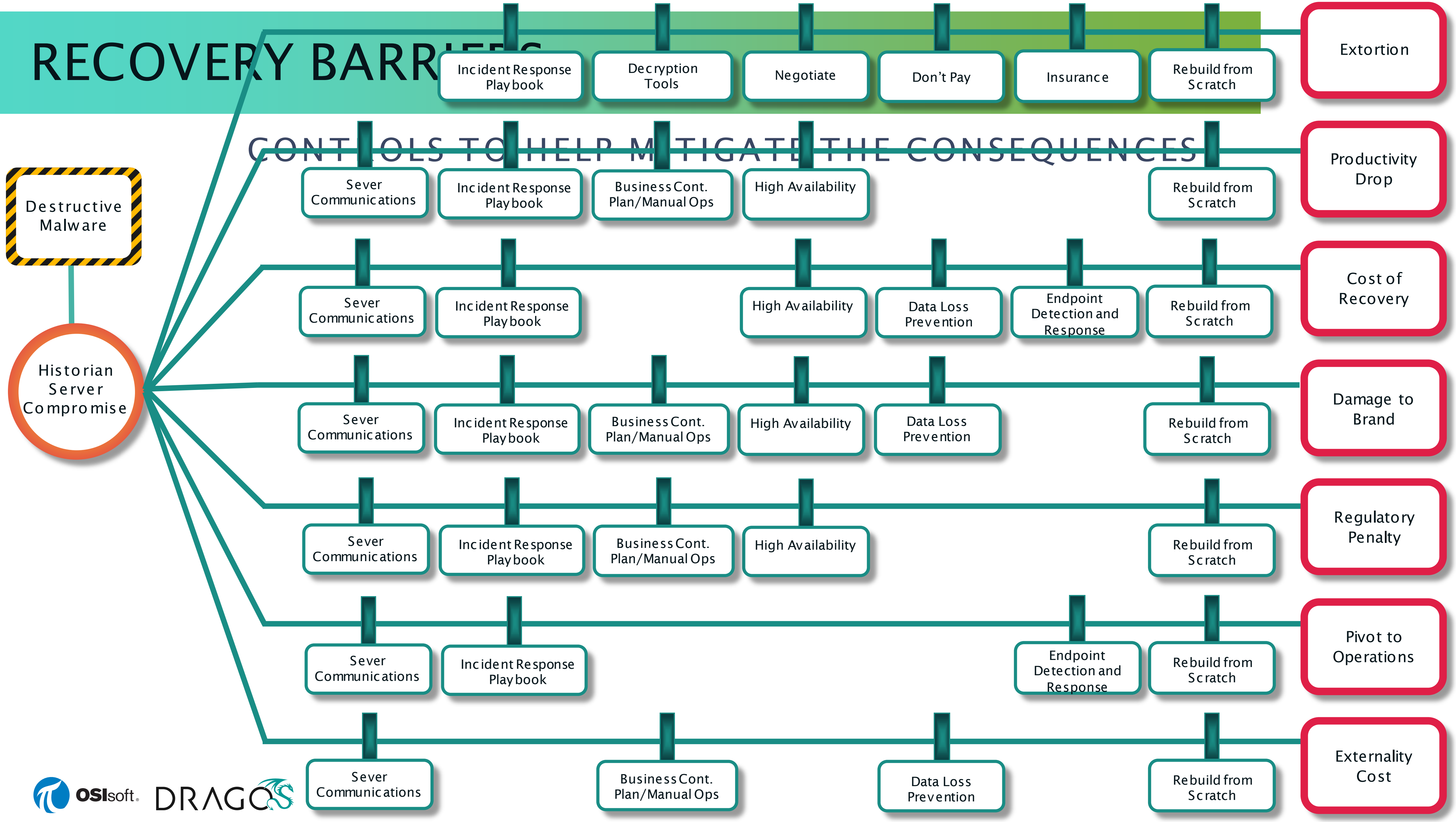
Externality Cost

Regulatory Penalty

Pivot to Operations

RECOVERY BARRIERS

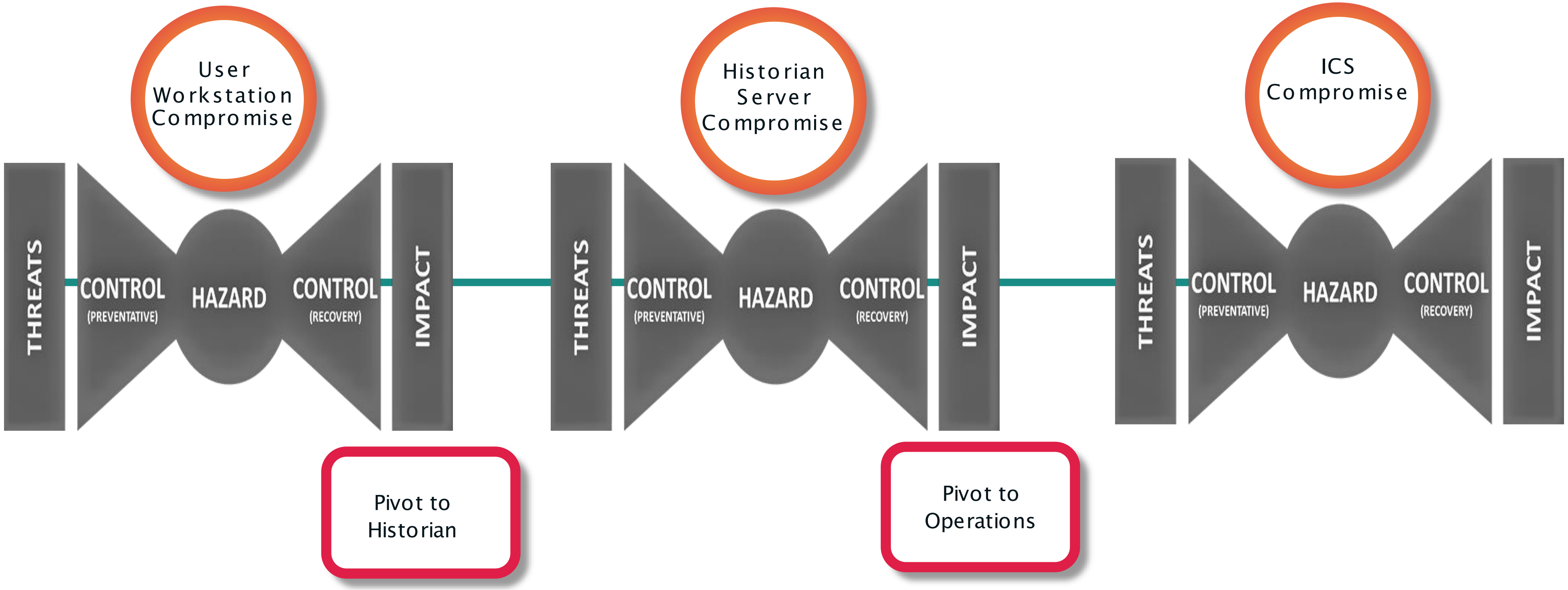
CONTROLS TO HELP MITIGATE THE CONSEQUENCES



OSIsoft DRAGOS

THE BOW TIE CHAIN

VISUALIZING FULL ATTACK PATHWAYS

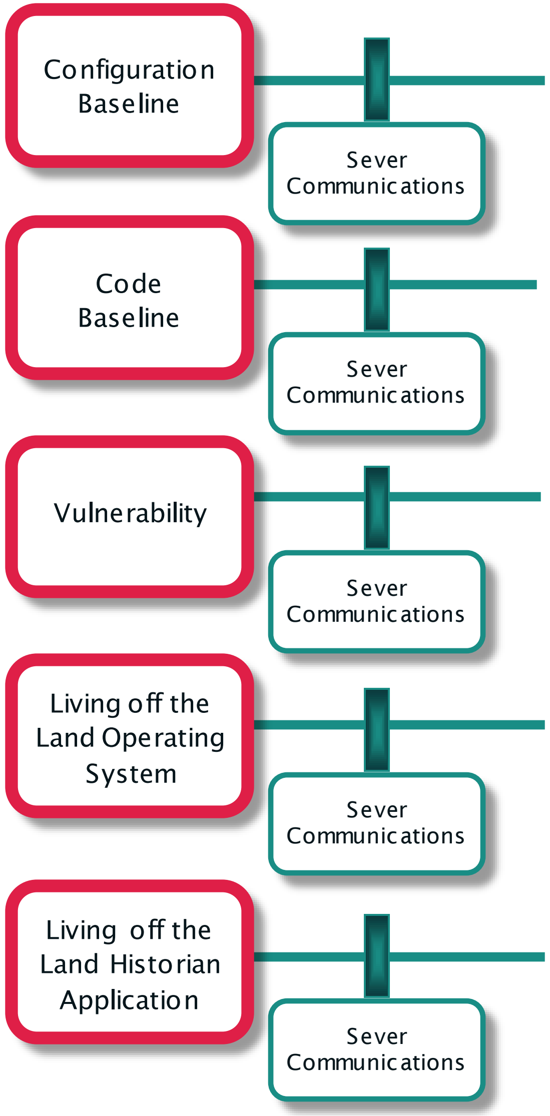


ANALYSIS HIGHLIGHTS – PREVENTION

THE DRAWBRIDGE

Sever Communications:

- Applicable to all threats and most consequences
- Aligns well with ISA/IEC 62443 Zones and Conduits
- Historians typically support degraded modes
- Highlighted despite short-lived effectiveness

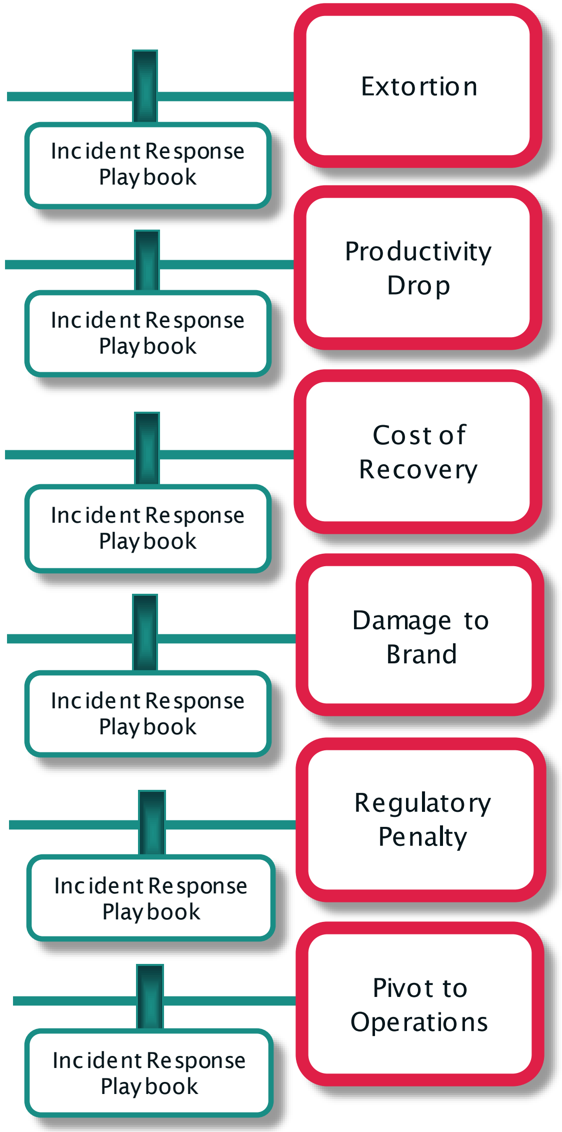


ANALYSIS HIGHLIGHTS – RECOVERY

FAIL TO PREPARE, PREPARE TO FAIL

Incident Response Playbook:

- Likely to reduce the overall impact should event occur
- Aligns with CISA's "Technical Approaches to Uncovering and Remediating Malicious Activity"
- Is the first step, can be further enhanced by running through a Tabletop Exercise (TTX)



ANALYSIS HIGHLIGHTS – RANSOMWARE

TO PAY OR NOT TO PAY

- The asset owner has a choice to make
- The decision should be rooted in safety, the organization's mission with consideration for legal and ethical obligations

FOLLOW-ON & CALL-TO-ACTION

HOW TO USE THIS INFORMATION AFTER TODAY

REAL LIFE APPLICATIONS & TAKEAWAYS

- Tabletop Exercises
  - Did we miss anything?
- Known incident comparison(s)
  - What lessons learned can be gleaned from your event or near miss
- Future Work
  - Please reach out for additional ideas and information

THANK YOU

A HUGE THANKS GOES TO..

Content and guidance

- Bryan Owen, OSIsoft
- Josh Carlson, Dragos

Marketing Support

- Blake Bisson, Dragos
- Mary-Grace Calosso, OSIsoft

RESOURCES

RECOMMENDED RESOURCES ON THIS TOPIC

PRESS RELEASES

Treasury Department Issues Ransomware Advisories to Increase Awareness and Thwart Attacks

113

October 1, 2020

Securing Data Integrity Against Ransomware Attacks:

Using the NIST Cybersecurity Framework and NIST Cybersecurity Practice Guides

THANK YOU

LMLCOCH@OSISOFT.COM
DMS@DRAGOS.COM

SIGNUP TO RECEIVE THE RECORDING AND SLIDES

To get the webinar recording and slides, please use this QR code or visit dragos.com/bowtie