



OSIsoft®

DRAGOS



**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

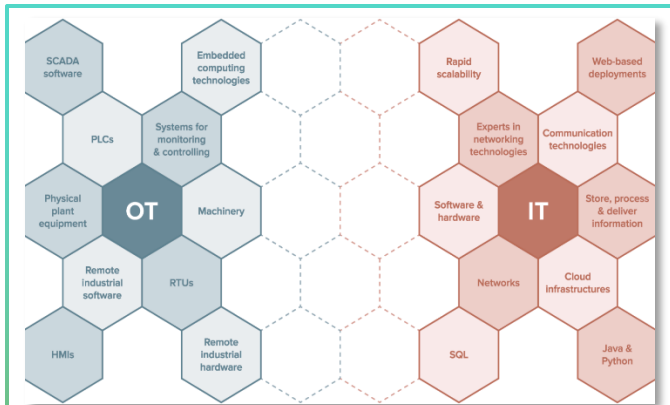
- + Industrial Pentester
- + ~3 years with Dragos
- + Before: Sempra Energy / SDG&E

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



USE CASE – RANSOMWARE

RAPIDLY EMERGING AS
THE MOST VISIBLE
CYBERSECURITY RISK.

LOTS OF LESSONS LEARNED
FROM RECENT INCIDENTS.





THE BOW TIE MODEL

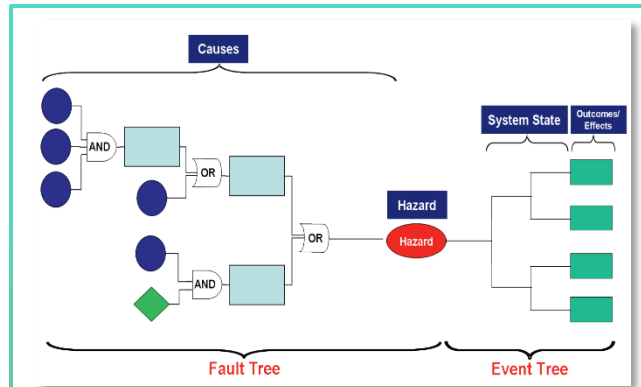
RISK ANALYSIS AND MODELING

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

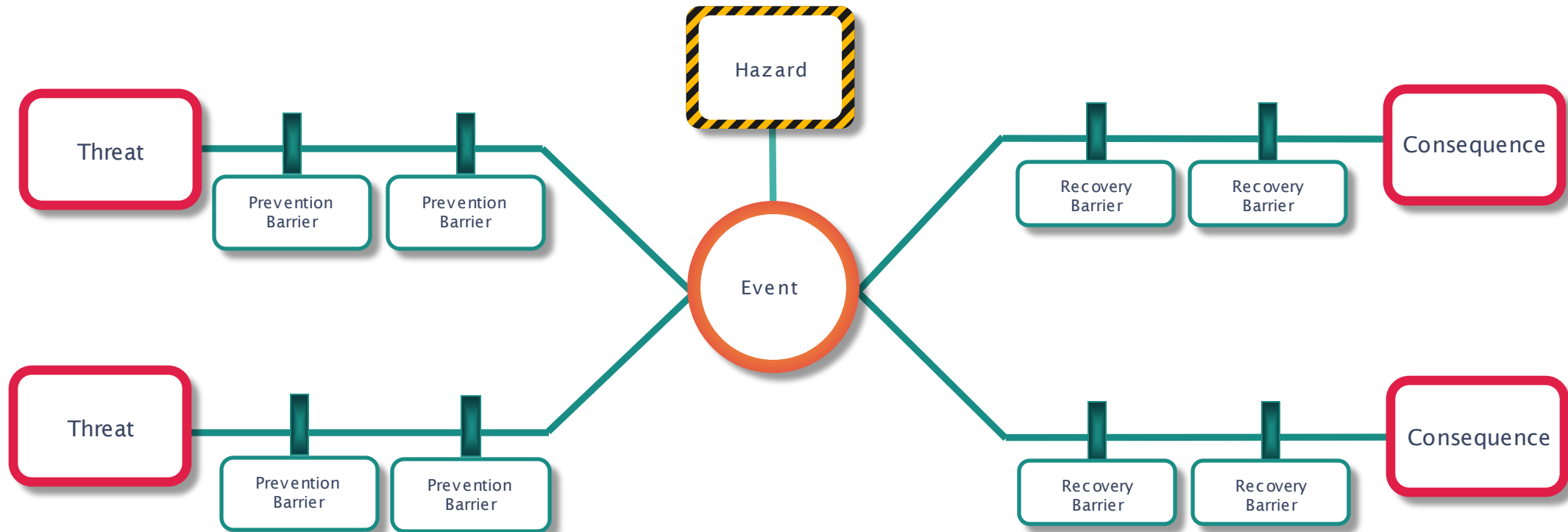
PROACTIVELY PROTECT TOMORROW			
RISK MANAGEMENT AND CYBERSECURITY GOVERNANCE <ul style="list-style-type: none"> Identify threats to the organization. Develop ICS cyber inventory of all hardware, software, and supporting infrastructure capabilities. Develop operational policy, procedures, training and awareness that address the specific capabilities of ICS. Develop and provide incident response procedures that align with ICS response processes. 	PHYSICAL SECURITY <ul style="list-style-type: none"> Limit user level access to and use of existing resources for those organizations with no power, remote, device access, and e-mail privileges. Enforce strict adherence to access controls to ensure that those ICS resources are not accessed by unauthorized users. Use multi-factor authentication, guards, and locks to control logical and physical access to ICS equipment and facilities. 	ICS NETWORK ARCHITECTURE <ul style="list-style-type: none"> Limit user level access to and use of existing resources for those organizations with no power, remote, device access, and e-mail privileges. Limit user level access to and use of existing resources for those organizations with no power, remote, device access, and e-mail privileges. Use multi-factor authentication, guards, and locks to control logical and physical access to ICS equipment and facilities. 	ICS NETWORK PERIMETER SECURITY <ul style="list-style-type: none"> Configure firewalls to control traffic between the ICS network and external networks. Limit IP geolocation as appropriate. Use the network access process to reduce risk to the network. Configure network devices to control security risks. Use all other network policies in order of priority to control security risks to the network. Configure all network devices to control security risks to the network.
HOST SECURITY <ul style="list-style-type: none"> Enforce a culture of patching and vulnerability management. Test all patches in a test environment before implementation. Implement application whitelisting or hardware-based controls. Support root device, including BIOS and UEFI firmware. Replace out-of-date software and hardware devices. Ensure critical data and services on ICS devices that need to remain available are backed up and recovery is tested. Configure exceptions and security for ICS protocols. 	SECURITY MONITORING <ul style="list-style-type: none"> Assess the baseline of normal operations and detect anomalies. Configure Intrusion Detection Systems (IDS) to detect anomalies. Use and monitor fault trees to detect anomalies. Use log security analysis and data mining (DAM) to analyze, analyze, and correlate events to detect anomalies. Configure ICS monitoring, security, and control when control is not a good option. 	SUPPLY CHAIN MANAGEMENT <ul style="list-style-type: none"> Align ICS procurement process to meet regulatory requirements. Configure ICS procurement process to meet regulatory requirements. Configure ICS procurement process to meet regulatory requirements. Configure ICS procurement process to meet regulatory requirements. 	HUMAN ELEMENT <ul style="list-style-type: none"> Have policies that define ICS security roles and responsibilities. Configure ICS security roles and responsibilities. Configure ICS security roles and responsibilities. Configure ICS security roles and responsibilities.

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



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



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



THE CONSEQUENCES

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

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



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

The background of the slide is a photograph of an industrial plant, possibly a refinery or chemical processing facility, with various towers, pipes, and scaffolding. A semi-transparent network of green lines and dots is overlaid on the top half of the image. A dark blue rectangular box with a thin green border is centered on the slide, containing the title text.

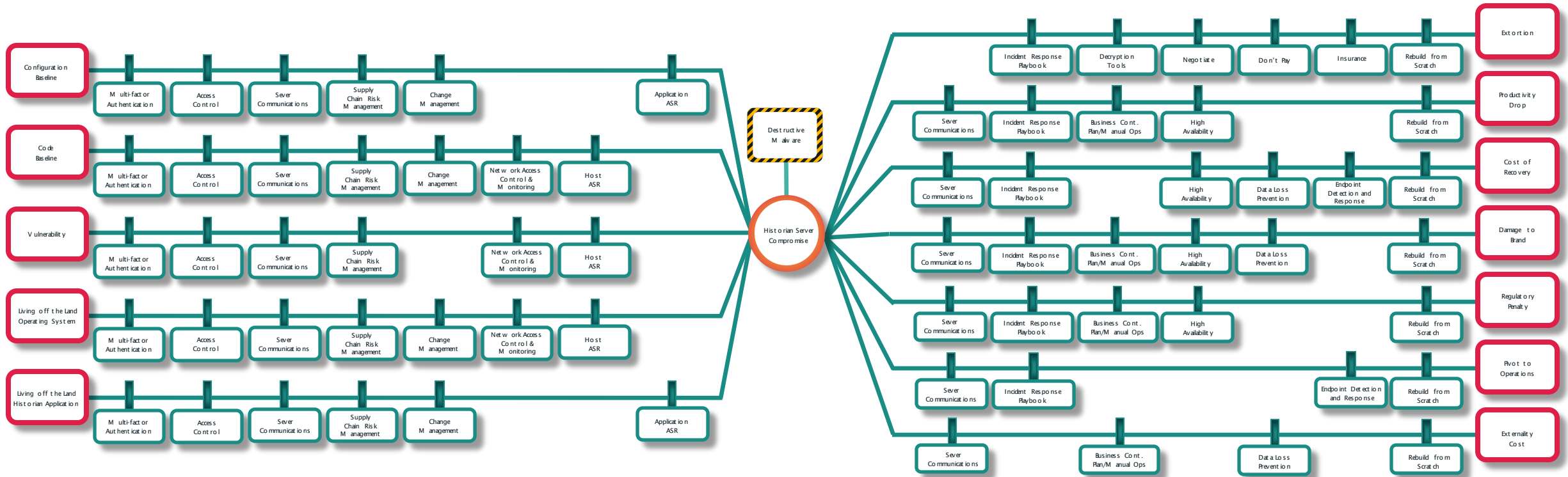
CASE STUDY: DESTRUCTIVE MALWARE ON ICS HISTORIAN

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

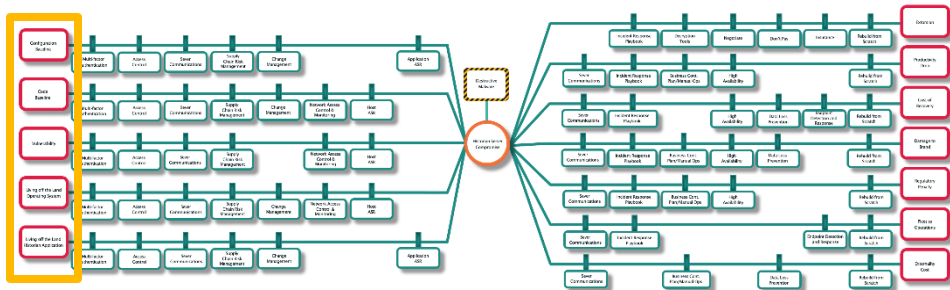




METHODOLOGY OVERVIEW – THREATS

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

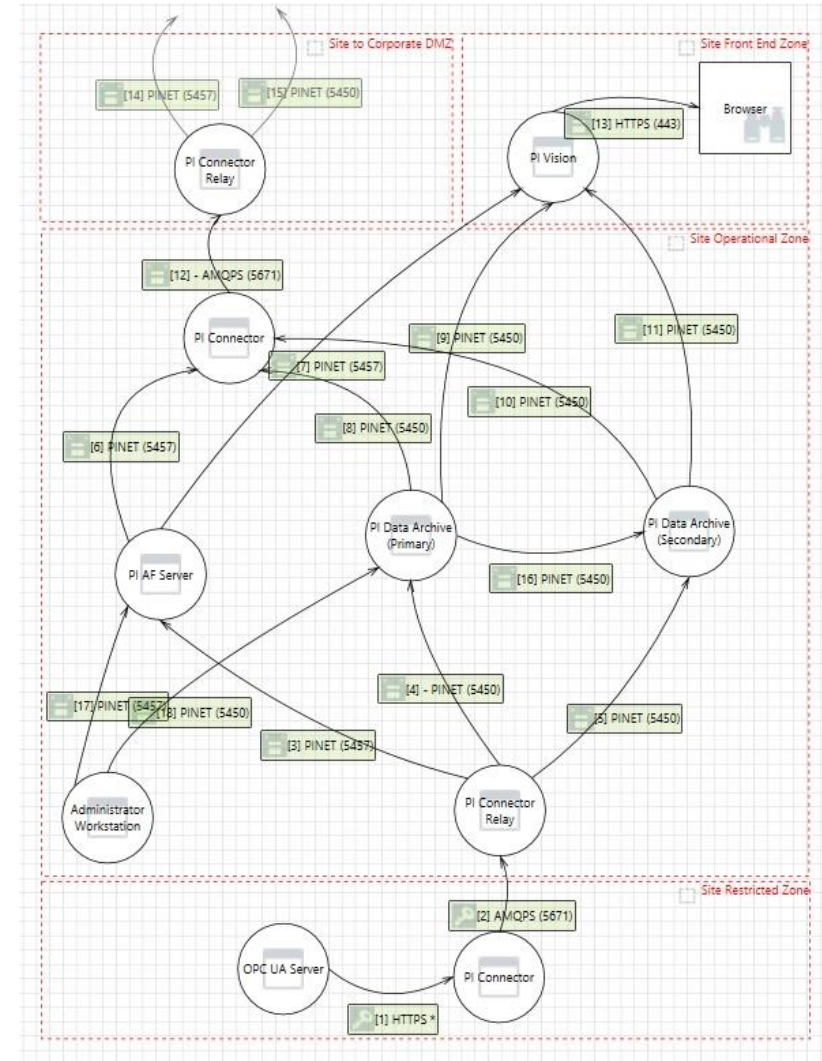
EPRI TECHNOLOGY ASSESSMENT METHODOLOGY

SYNERGY BETWEEN EPRI TAM AND BOW TIE MODELS



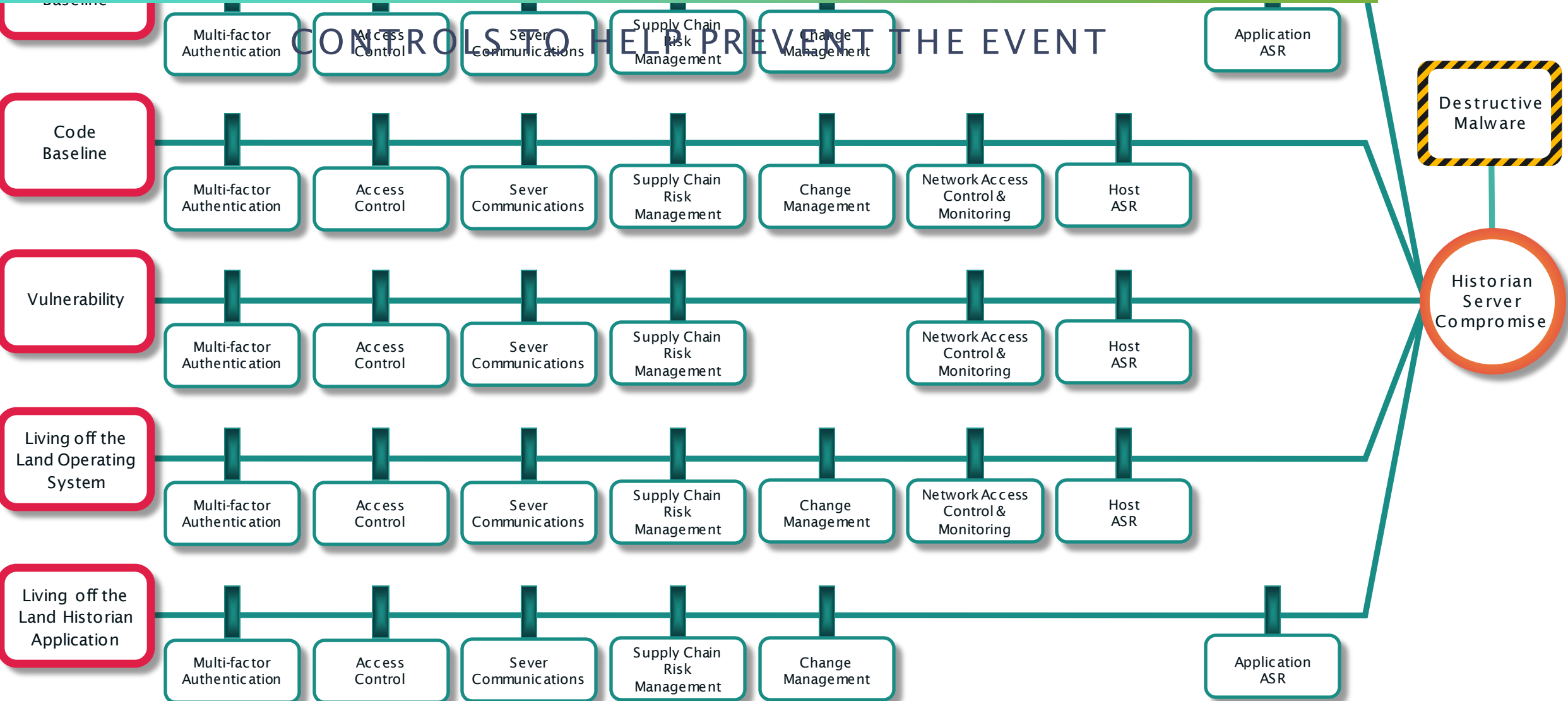
Cyber Security Technical Assessment Methodology

Risk Informed Exploit Sequence Identification and Mitigation, Revision 1

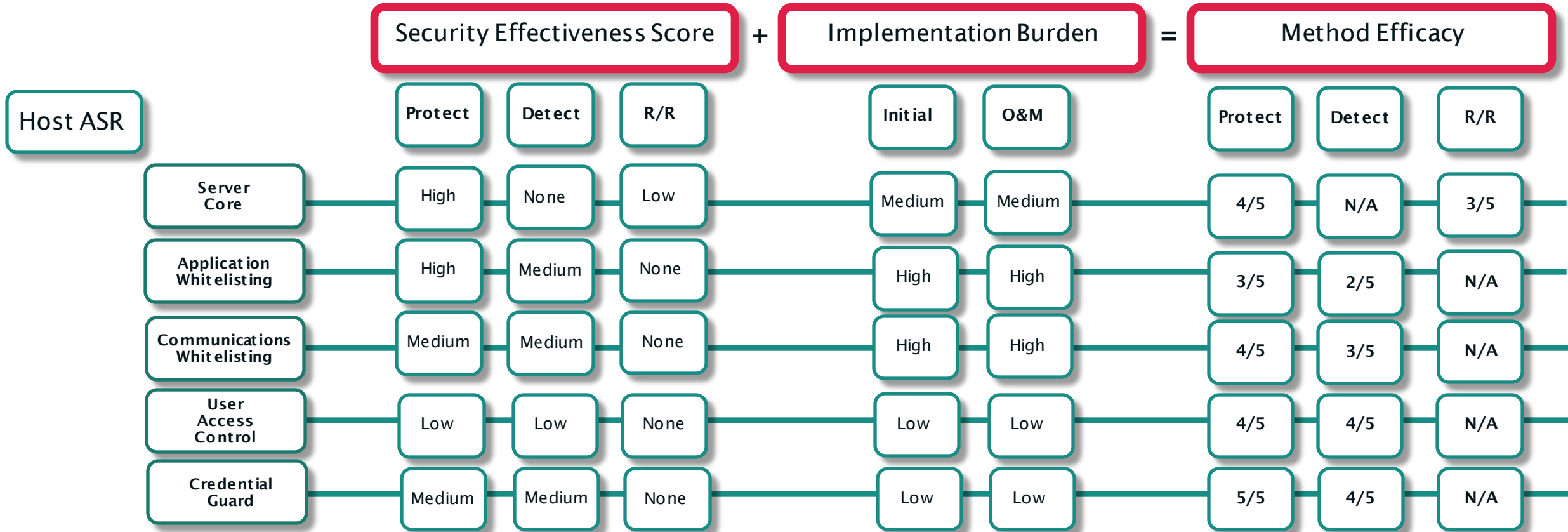


PREVENTION BARRIERS

CONTROLS TO HELP PREVENT THE EVENT



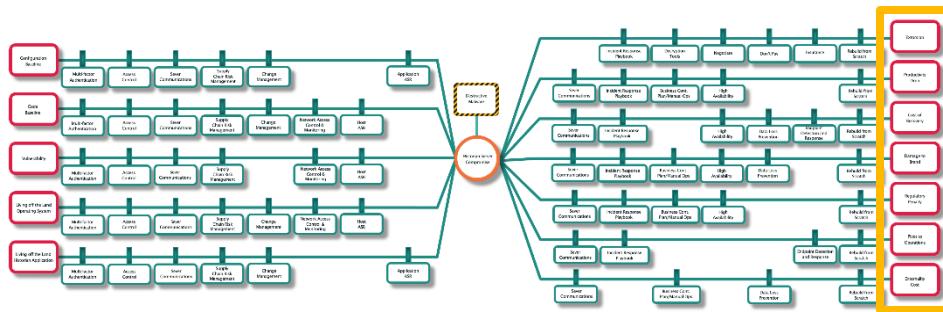
DEEP DIVE INTO A PREVENTION BARRIER



METHODOLOGY OVERVIEW – CONSEQUENCES

INSPIRATION AND FOUNDATIONAL CONCEPTS

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



RECOVERY BARRIERS

CONTROLS TO HELP MITIGATE THE CONSEQUENCES



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

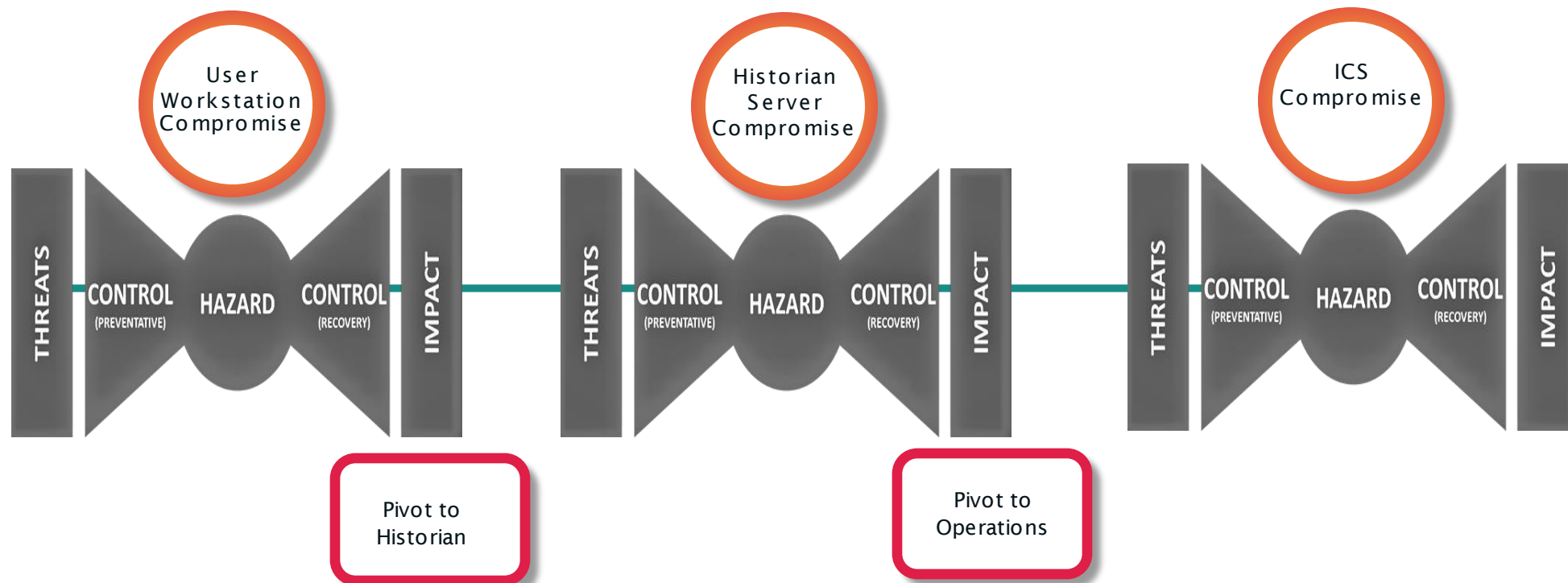
Data Loss Prevention

Rebuild from Scratch

Externality Cost

THE BOW TIE CHAIN

VISUALIZING FULL ATTACK PATHWAYS

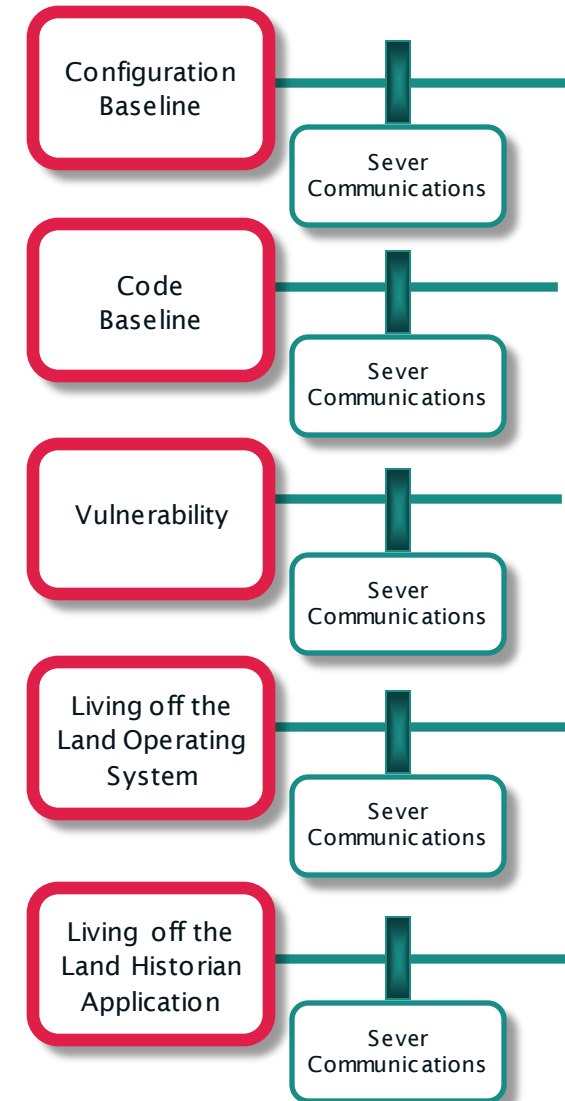


ANALYSIS HIGHLIGHTS – PREVENTION

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

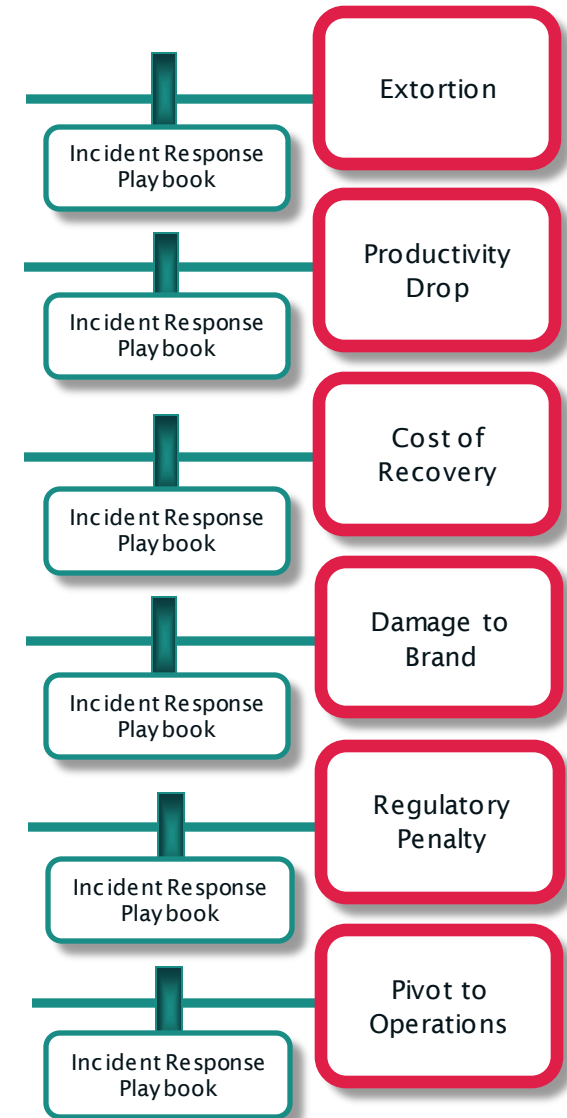


ANALYSIS HIGHLIGHTS – RECOVERY

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

The background features a complex industrial scene with large, metallic pipes and machinery. The color palette is dominated by shades of green and black. Overlaid on the image are various technical graphics, including circuit-like lines, gears, and arrows, suggesting a focus on engineering or technology. A central black rectangle with a thin green border contains the word "RESOURCES" in a bold, green, sans-serif font.

RESOURCES

RECOMMENDED RESOURCES ON THIS TOPIC



PRESS RELEASES

Treasury Department Issues Ransomware Advisories to Increase Awareness and Thwart Attacks



October 1, 2020

ATTACK SURFACE REDUCTION

MICROSOFT DEFENDER
ADVANCED THREAT PROTECTION



Stopping Shadow Copies - A Second
Look Into Deletion Methods



Securing Data Integrity Against Ransomware Attacks:

Using the NIST Cybersecurity Framework and NIST Cybersecurity Practice Guides

The background features a faded industrial scene with tall distillation columns and a complex network of pipes. A semi-transparent network of green lines and dots is overlaid on the top half of the image. A large black rectangle with a thin green border is centered in the middle, containing the text 'THANK YOU' in a light green, sans-serif font.

THANK YOU

LMLCOCH@OSISOFT.COM
DMS@DRAGOS.COM



OSIsoft®

DRAGOS 

SIGNUP TO RECEIVE THE RECORDING AND SLIDES

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

