Whitepaper

Using Bow Tie Risk Modeling for Industrial Cybersecurity

Josh Carlson | Dragos, Inc.
Daniel Michaud-Soucy | Dragos, Inc.
Bryan Owen PE | OSIsoft, now part of AVEVA
Lubos Mlcoch | OSIsoft, now part of AVEVA

info@dragos.com
@DragosInc

TABLE OF CONTENTS

I. INTRODUCTION

Bow tie diagrams are a proven and effective way to quickly understand industrial hazards. When applied to the cybersecurity realm, bow tie risk analysis and modeling can provide an ideal method for visualizing cybersecurity risk. With a well-crafted bow tie model, cybersecurity defenders and executives can glean important insights that will help them prioritize defensive measures and more effectively improve their security posture over time.

What is Bow Tie Modeling?

Bow tie risk analysis is a method of risk assessment with deep roots in several industrial verticals. It's been utilized for more than four decades in highly hazardous chemical environments and came to prominence in the oil and gas industry following the Piper Alpha incident of 1988 when the Shell group adopted it to better understand hazards and risks in the field. The methodology combines several types of risk analysis, including fault tree analysis, event tree analysis, and causal factors charting. Bow tie modeling takes a threats and consequences approach to visualizing risk. This visualization makes it easier to identify controls that can be used both on the preventative side to minimize the likelihood of threats causing a specific undesirable event and on the recovery side to minimize the severity of consequences when that event does occur. Dragos has long advocated for a threats-and-consequences approach to cybersecurity risk assessment. We believe this approach using bow tie methodology will be increasingly applied as a common lens for viewing cybersecurity risk and industrial process hazard analysis.

How Bow Tie Modeling Can Be Powerful for Cybersecurity

Based on that belief, Dragos embarked on a long-term collaboration with experts from the industrial software company OSIsoft, now part of AVEVA, to establish a normalized method for bringing the bow tie to bear on cyber scenarios. OSIsoft makes the PI System, the leading operations data management platform in essential sectors. Together the collaborative team put months of work into a version of bow tie modeling that would work well for cybersecurity. We're committed to this work because we believe the bow tie could provide a powerful tool for operational technology (OT) cybersecurity for several reasons:

- **To bridge the OT-IT cybersecurity gap:**
  Bow tie modeling is technology and environment agnostic, meaning it can be applied on both IT and OT cybersecurity events and can serve to tap expertise in both domains.
- **To model new cyber risks during digital transformation:**
  Bow tie modeling can be used to readily assess hazards and events that could impact new technology implementations in operational environments.
- **To conduct more effective tabletop exercises:**
  Bow tie modeling serves as an excellent tool for cybersecurity and business continuity teams to gain a better understanding of their incident response readiness for the events that could have the most severe consequences.

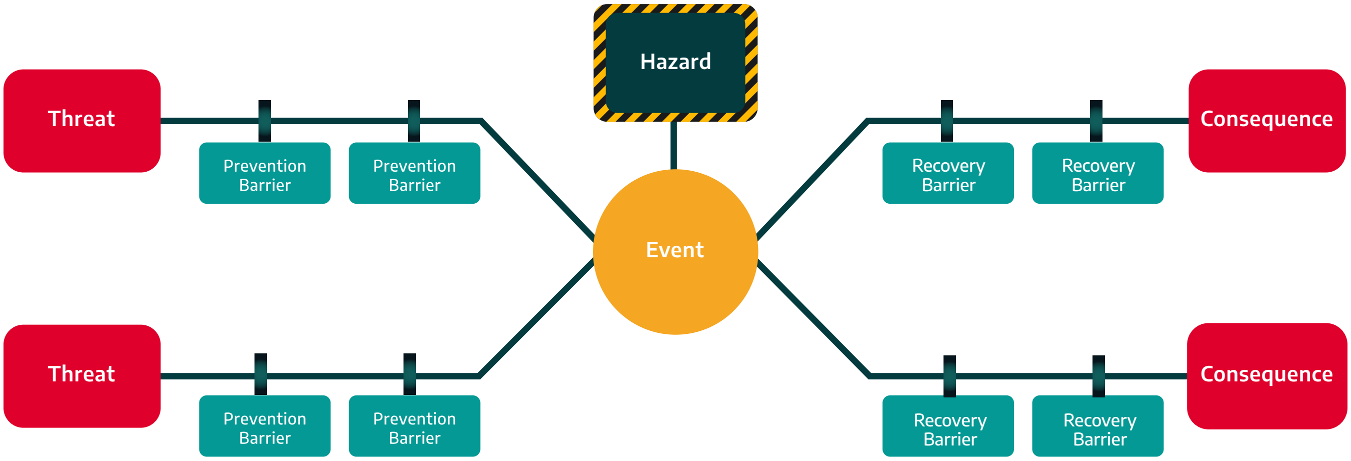
- **To plan controls roadmaps around threats and consequences:** Bow tie modeling offers both at-a-glance and in-depth insights about important defenses as well as potential single points of failure with a path to consequences that impact business operations.

Finally, as an established risk assessment method that is grounded in industrial safety, many operational engineers are familiar with bow tie modeling. When applied to cyber-security events, bow tie is an ideal method to help narrow the cultural divide between cybersecurity professionals and operations staff.

II. UNDERSTANDING BOW TIE BASICS

Before delving into the mechanics of leveraging the bow tie for cybersecurity, let's set a baseline to understand the basics of how bow tie risk analysis and modeling works.

Briefly, here's a mockup of the main components in a basic bow tie model:



The center knot of the bow tie is the identified event that the organization is trying to manage risks around. To the left are preventative factors related to potential threats that can trigger the event to occur. To the right are factors that can reduce adverse outcomes if the event actually happens.

To help explain the basics of how this works, we'll describe the main components of a bow tie model in an Oil and Gas context.

The Knot

At the center of the model is the ‘knot,’ which is pinned to the risk which an organization has identified as important to manage.

Hazard
The first piece of the knot is the hazard. It’s the environmental condition which organizations must deal with day-in and day-out. At the industrial facility level, the hazards are obvious—they’re things that smash, things that shock, dangerous chemicals, and so on. Such hazards are the things that need to be controlled to prevent bad things from happening.

⚠ **HAZARD EXAMPLE:**
The operation of a fluid catalytic cracker (FCC) in a petroleum refinery.

Event
While the hazard is the environmental context, the event is the bad thing that an organization is trying to prevent from happening or at least trying to limit the impact if it does occur. It is what happens when the control over the hazard is lost.

⚠ **EVENT EXAMPLE:**
The formation of an uncontrolled explosive atmosphere within the FCC unit.

The Left Side

The left side of the model are considerations made before an event occurs to keep it from happening.

Threats
The threats are whatever factors that have the potential to cause the identified event to happen.

⚠ **THREAT EXAMPLE:**
The backward flow of a flammable hydrocarbon mixture to the air-side of the FCC from the reactor, through the regenerator, and into the electrostatic precipitator (ESP).

Prevention Barriers
The prevention barriers are controls put in place to interrupt identified threats so that they neutralize situations that could lead to the event happening.

⚠ **PREVENTION BARRIER EXAMPLE:**
Slide valves separating the reactor and the regenerator.

The Right Side

The right side of the model are preparations made so that if an event does occur, the organization can attempt to prevent, or at least minimize, the severity of negative consequences from impacting the Industrial Control System (ICS) environment.

Consequences
The consequences are potential outcomes that could cause negative impacts for the business or the safety of people.

CONSEQUENCES EXAMPLE:
Explosion of the system.

Recovery Barriers
Recovery barriers limit the escalation of the event scenario to mitigate identified negative impacts.

RECOVERY BARRIER EXAMPLE:
Steam barrier deployed to pressurize the reactor above the main column pressure to isolate the two sides.

III. APPLYING BOW TIE MODELING

To start applying bow tie modeling to cybersecurity scenarios, Dragos and OSIsoft went through a process of collaboration and rapid ideation for a model centered around the risks of destructive malware on ICS historian servers. Each side of the team brought to bear very different practitioner perspectives in a multi-month analysis that was informed by actual incidents and near misses of historian server compromises caused by destructive malware.

The modeling methodology is still a work in progress, and both firms encourage other industry collaborators to provide feedback to help us continually improve on this model for the good of practitioners worldwide.

The Knot

Hazard
Our example cybersecurity bow tie model is pinned to the hazard of destructive malware, such as ransomware like EKANS, which contains built-in, ICS-specific functions and offers a prime example of the growing kinds of risk that stems from this hazard.

Event
The event identified in this working model is the compromise of an ICS data historian server by a cyber attacker.

SOURCE: Cyber Security Technical Assessment Methodology (TAM) from the Electric Research Power Institute (EPRI). https://www.epri.com/research/products/000000003002012752

The Left Side

The left side of our cybersecurity bow tie model is informed by the Cyber Security Technical Assessment Methodology (TAM) from the Electric Research Power Institute (EPRI).

Threats

Our modeling work led us to identify five major threats that could lead to destructive malware being able to compromise a historian server. The descriptive titles are based on EPRI TAM terminology.

- **Configuration Baseline:**
  A threat actor using the malware to make unauthorized configuration changes to the system to compromise it.
- **Code Baseline:**
  A threat actor triggering unauthorized code execution to achieve compromise and control over the system.
- **Vulnerability:**
  A threat actor taking advantage of software bugs including 'zero day' issues with the software to take over the system.
- **Living off the Land - Operating System:**
  A threat actor leveraging built-in features or tools in the operating system used for maintenance or administration to carry out the attacks. For example, by exploiting PowerShell in a Windows operating system.
- **Living Off the Land - Historian Application:**
  Similarly, a threat actor leveraging built-in tools within the historian itself to further an attack.

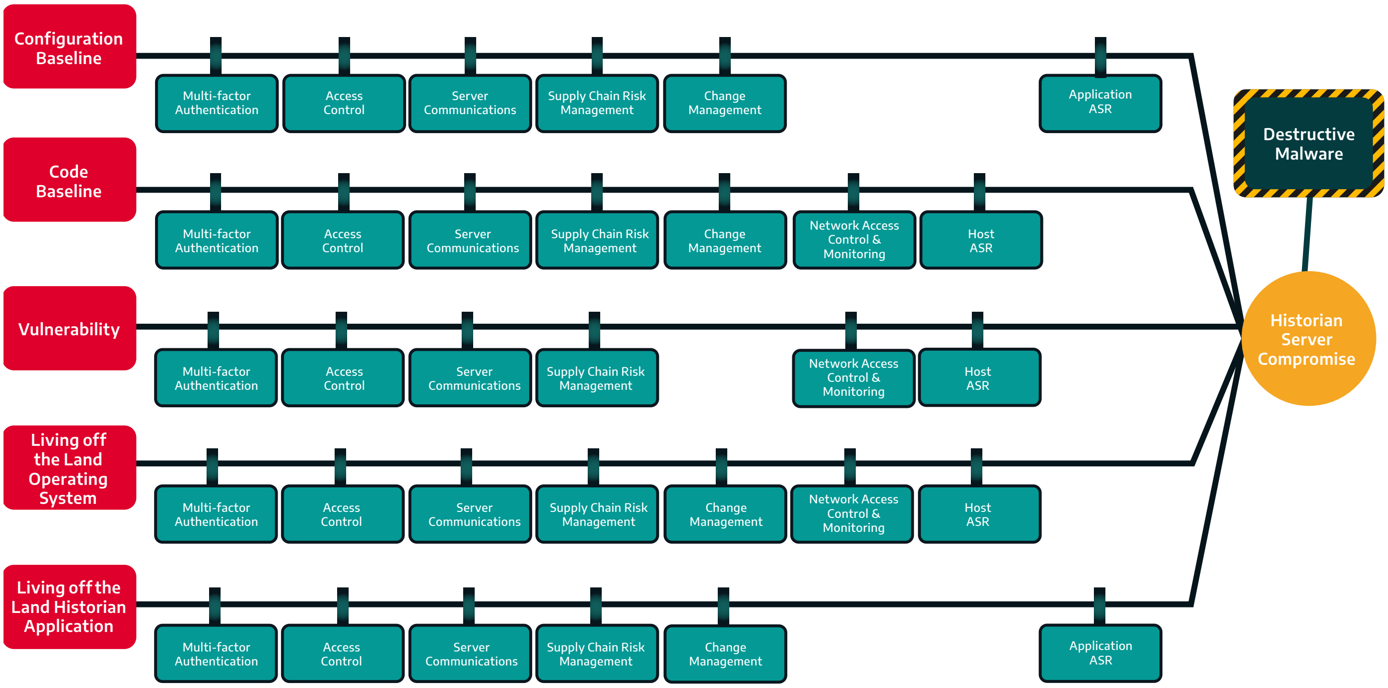
The Prevention Barriers

For each threat scenario, we identified six to seven prevention barriers that could help prevent the threat from ultimately triggering the event. Four of them were controls that could act as a barrier in every single scenario: multi-factor authentication, access control, server communications, and supply chain risk management. Then we had a smaller set of barriers that were effective against most of the threats, or at least just a few of them, such as Host Attack Surface Reduction (ASR).

	Security Effectiveness Score			Implementation Burden		Method Efficacy		
Host ASR	Protect	Detect	R/R	Protect	Protect	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

The barriers we identified can be mapped directly into existing cybersecurity frameworks, such as the MITRE ATT&CK framework mitigations. For example, the multi-factor authentication barrier can be mapped to M1032. And access control could be mapped to multiple ATT&CK mitigations, including privileged account management (M1026), user account management (M1018), and credential access protection (M1043).

SOURCE: MITRE ATT&CK https://collaborate.mitre.org/attackics/index.php/MainPage


Configuration Baseline
Multi-factor Authentication
Access Control
Server Communications
Supply Chain Risk Management
Change Management
Application ASR
Code Baseline
Multi-factor Authentication
Access Control
Server Communications
Supply Chain Risk Management
Change Management
Network Access Control & Monitoring
Host ASR
Vulnerability
Multi-factor Authentication
Access Control
Server Communications
Supply Chain Risk Management
Network Access Control & Monitoring
Host ASR
Living off the Land Operating System
Multi-factor Authentication
Access Control
Server Communications
Supply Chain Risk Management
Change Management
Network Access Control & Monitoring
Host ASR
Living off the Land Historian Application
Multi-factor Authentication
Access Control
Server Communications
Supply Chain Risk Management
Change Management
Application ASR
Destructive Malware
Historian Server Compromise

Efficacy scores in the example above are simulated to illustrate how the modeling process would work. Actual scoring requires organization-specific context. Efficacy scoring should be performed based on individual ICS environments, as well as existing cybersecurity programs, policies, and so on. The point to understand is that this scoring methodology considers security effectiveness for protection, detection, as well as response and recovery from an event. It also considers implementation costs, both initial and ongoing. Putting those two items together helps develop a score for the overall method efficacy of the barrier in whatever domains that it operates.

The Right Side

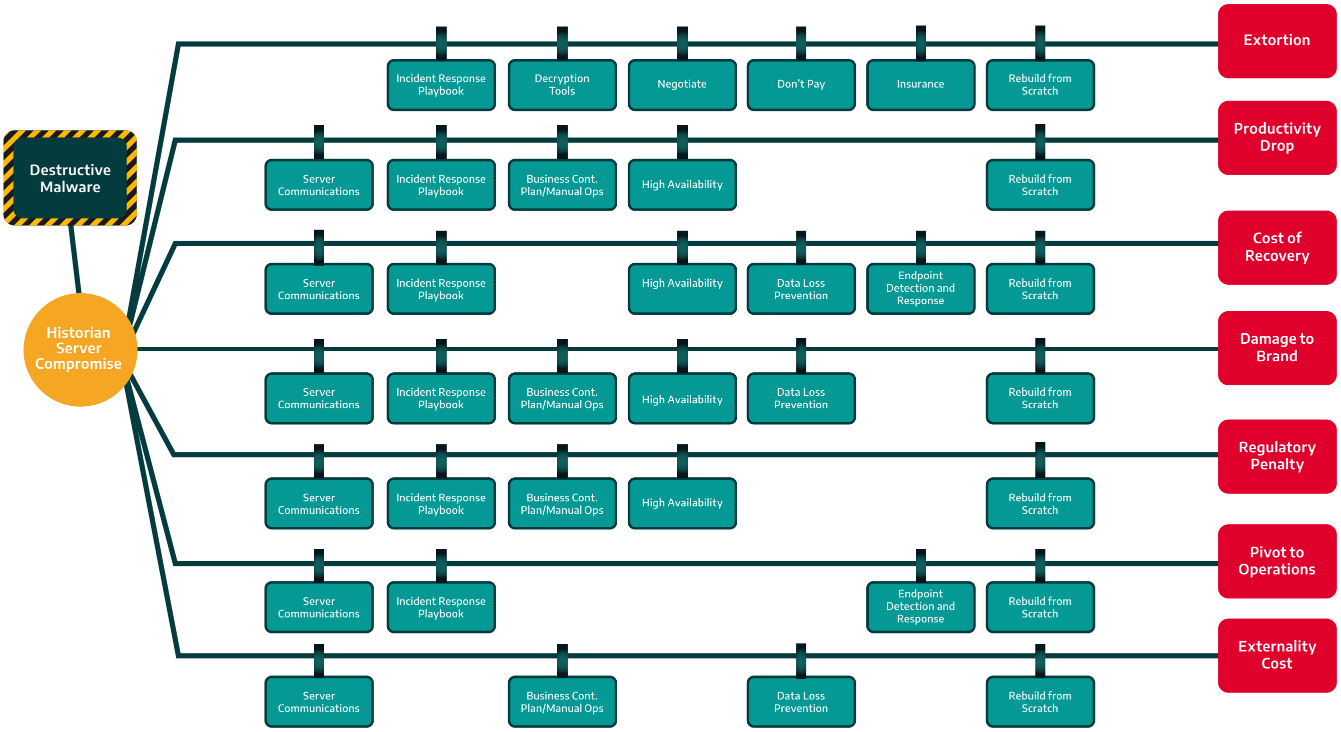
As we explained in the simple example above, the right side of the bow tie assumes that the event has already occurred. The prepared recovery barriers identified are meant to minimize consequences. In developing this part of the cyber bow tie model, we leaned heavily on the Factor Analysis of Information Risk (FAIR) loss model categories to inform our work.

Consequences

Our team identified seven major consequences that could cause negative impacts based on the historian server compromise event. Most of these come from FAIR, which covers impacts like productivity drop, cost of recovery, and damage to the brand. Additionally, since one of our hazards includes ransomware, we felt it was crucial to add extortion to the mix. We also added externality cost, which is important when an organization provides critical services, such has been the case with pipeline operators falling victim to ransomware.

Recovery Barriers

As you inspect the right side of the diagram, it becomes clear that even when the event happens, there are a lot of preparations that organizations can make to mitigate the impact of the event or prevent escalation to the actual consequences identified here.



As with prevention barriers, there are several recovery barriers that provide mitigation for multiple consequence categories, such as severing communications, incident response playbooks, and business continuity planning.

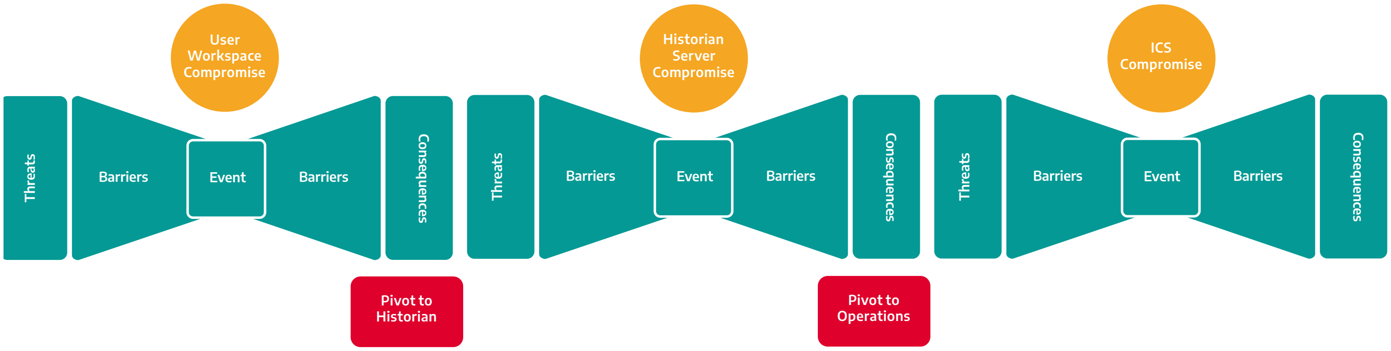
To understand how the analysis of these barriers works within the bow tie model, let us think about one unique barrier that cuts across every threat and almost all consequences: severing communications. Doing so is like defenders retracting drawbridges to protect a medieval city and its citizens. Severing communications is a control that may have strong but very short-term effectiveness and limits the overall effectiveness of historian operation.

Just as retracting a drawbridge puts a city under siege and limits how it operates, severing communications degrades how the application performs. So, understanding how and *when* to activate this measure is crucial. This recovery barrier limitation highlights exactly why multiple barriers are needed to fully mitigate a consequence from coming to realization.

IV. VISUALIZING FULL ATTACK

Obviously, the bow tie model described here centers on one single event. As organizations begin to develop their own cyber bow tie models, they will soon find that the real power of this methodology for cybersecurity scenarios is how these models can link together to start to predict interrelated events and system pivots by attackers. Putting together a chain of bow ties can help an organization visualize the extent of ICS attack pathways and important defenses in the chain.

For example, the attack chain may originate initially with a user workstation compromise, which would then be used to pivot to a historian compromise. That compromise could also be used to trigger a further event which would be a complete compromise of the ICS.



Just by looking at this chain of bow ties visually can help decision-makers identify attacker pivot points and associated defensive barriers to thwart the spread of destructive malware.

V. NEXT STEPS FOR PRACTITIONERS

We observe increasing numbers of cybersecurity practitioners starting to apply bow tie methodology to elevate their OT cybersecurity strategy.

Constructing your own bow tie models can really enable organizations to hold discussions and tabletop exercises between distinct groups of people—be it cybersecurity, business leaders, ops managers, or IT staff. This makes it easier to plan for incidents and start to brainstorm ways to overcome critical control gaps in a prioritized way. When practitioners facilitate these brainstorming sessions, we recommend keeping them short and to start by collecting ideas that stick when it comes to imagining worst-case scenarios. From there, you can identify prevention and recovery barriers and start coalescing them into a compelling visual model.

As organizations develop these models, they can start to link them to known or past events or even near-miss events. This method can be useful to not only prove the value of the bow tie model itself but to also visualize the attack pathway that led to the incident or near-miss.

Bow tie diagrams help build a common understanding of security events and barriers appropriate for your organization—even for complex industrial cybersecurity hazards.

For more in-depth technical information about the work done by Dragos and OSIsoft, check out our informative webinar featuring the minds behind this cyber model: **www.dragos.com/bowtie**