DRAGOS

Starting Your Journey

A Roadmap for ICS/OT Security

Jason D. Christopher
Director of Cyber Risk

JASON D. CHRISTOPHER

Director of Cyber Risk

DRAGOS

@jdchristopher

in linkedin.com/in/jdchristopher

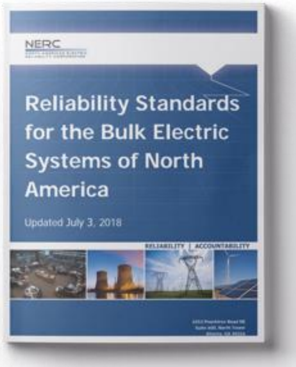
- Cyber risk management professional services, tied to threat intel & Dragos platform
- Certified SANS Instructor for industrial control systems security
- Former CTO for Axio Global, Inc., leading critical infrastructure protection strategy
- Federal energy lead for several industry standards and guidelines, including NERC CIP, NIST CSF, and the C2M2
- Led cyber incident & risk management team for US Department of Energy
- Security metrics development across EPRI and other research organizations
- Began career deploying & securing ICS
- Frequent speaker at conferences & client events
- MS, Electrical Engineering, Cornell

ELECTRICITY CYBERSECU

OIL AND NA CYBERSECUR

CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2)

Version 1.1
February 2014



NERC

Reliability Standards for the Bulk Electric Systems of North America

Updated July 3, 2018

RELIABILITY | ACCOUNTABILITY

Incentivizing Cyber Security: A Case for Cyber Insurance

Written by Jason D. Christopher

June 2017

DEPARTMENT OF ENERGY FEDERAL ENERGY REGULATORY COMMISSION

DEPARTMENT OF ENERGY UNITED STATES OF AMERICA

axio

SANS

EPRI ELECTRIC POWER RESEARCH INSTITUTE

Today’s Discussion

Roadmapping 101

Some initial questions

Every journey starts somewhere– but do you know where you are going? What’s important? And how to begin?

Deviously “Simple” Roadmap

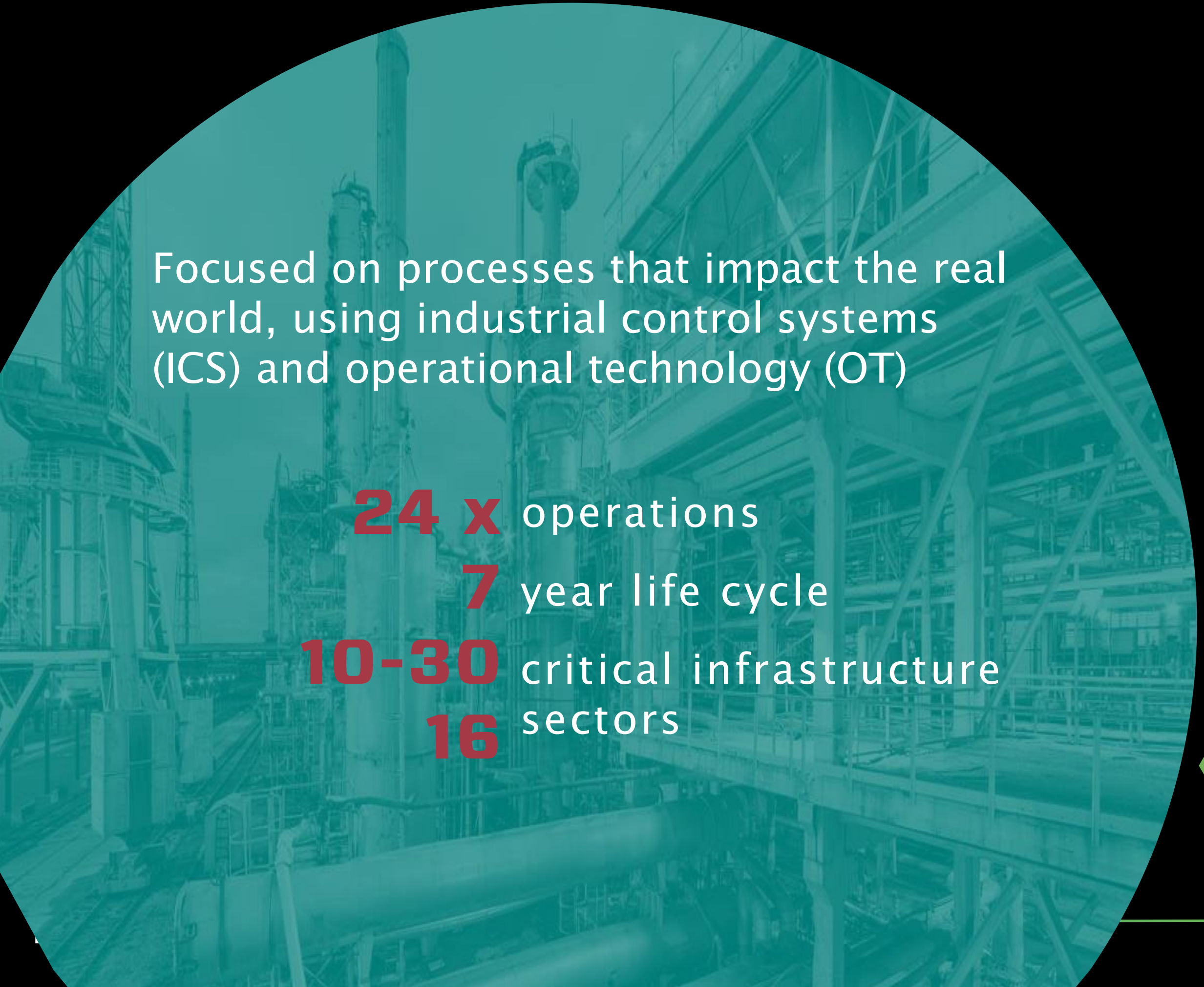
Cutting down the steps to establish a repeatable, measurable process for ICS/OT security program improvement.

Use case

Real world and applicable discussions for roadmap creation and timelines.

ICS/OT = Industrial Operations

Protecting what matters most



Focused on processes that impact the real world, using industrial control systems (ICS) and operational technology (OT)

24 x operations

7 year life cycle

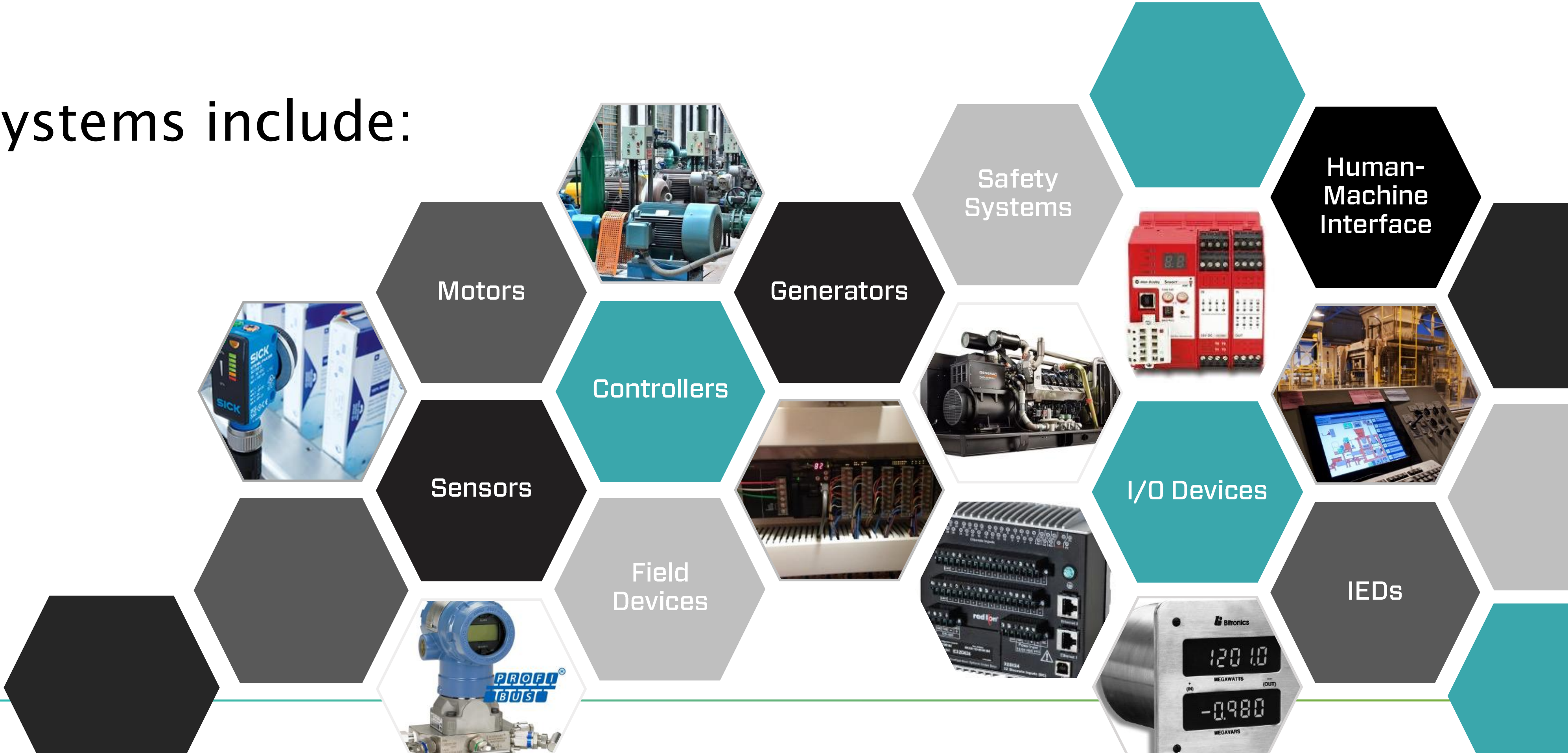
10-30 critical infrastructure

16 sectors

What do we mean by ICS/OT?

When a 0 or 1 impacts the physical world.

Devices and systems include:



Safety Systems

Human-Machine Interface

Motors

Generators

Controllers

Sensors

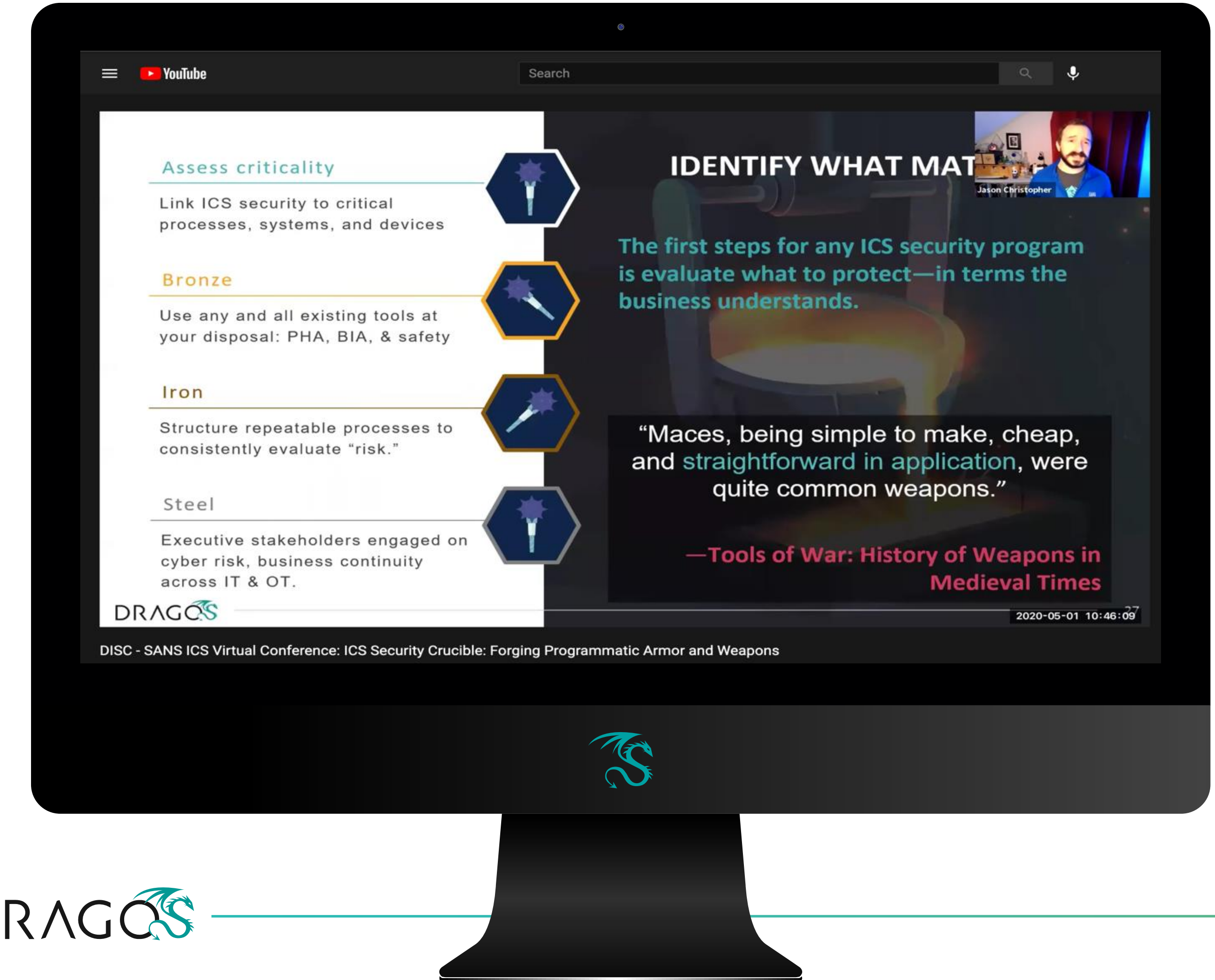
I/O Devices

Field Devices

IEDs

Not the first time…

Other presentations on “starting”



Assess criticality

Link ICS security to critical processes, systems, and devices

Bronze

Use any and all existing tools at your disposal: PHA, BIA, & safety

Iron

Structure repeatable processes to consistently evaluate “risk.”

Steel

Executive stakeholders engaged on cyber risk, business continuity across IT & OT.

IDENTIFY WHAT MAT

The first steps for any ICS security program is evaluate what to protect—in terms the business understands.

> “Maces, being simple to make, cheap, and straightforward in application, were quite common weapons.”
>
> —Tools of War: History of Weapons in Medieval Times

2020-05-01 10:46:09

DISC - SANS ICS Virtual Conference: ICS Security Crucible: Forging Programmatic Armor and Weapons

Way, way back… in 2020

- Explored the ICS Security Crucible
- Built a starting point and assess maturity for *any* OT security program
- Used medieval weapons

https://hub.dragos.com/on-demand/sans-virtual-ics-security-crucible

By 2023, ***75% of organizations will restructure risk and security governance*** to address converged IT, OT, Internet of Things (IoT), and physical security needs, an ***increase from fewer than 15%*** in 2021.

– Gartner

Why now?

Workforce

Growing base of skilled ICS security practitioners in need of team leaders and managers

Governance

Boards and executives increasingly highlight industrial cyber risk as a top concern

Projects

Increased connectivity in technology deployments requiring ICS security project management

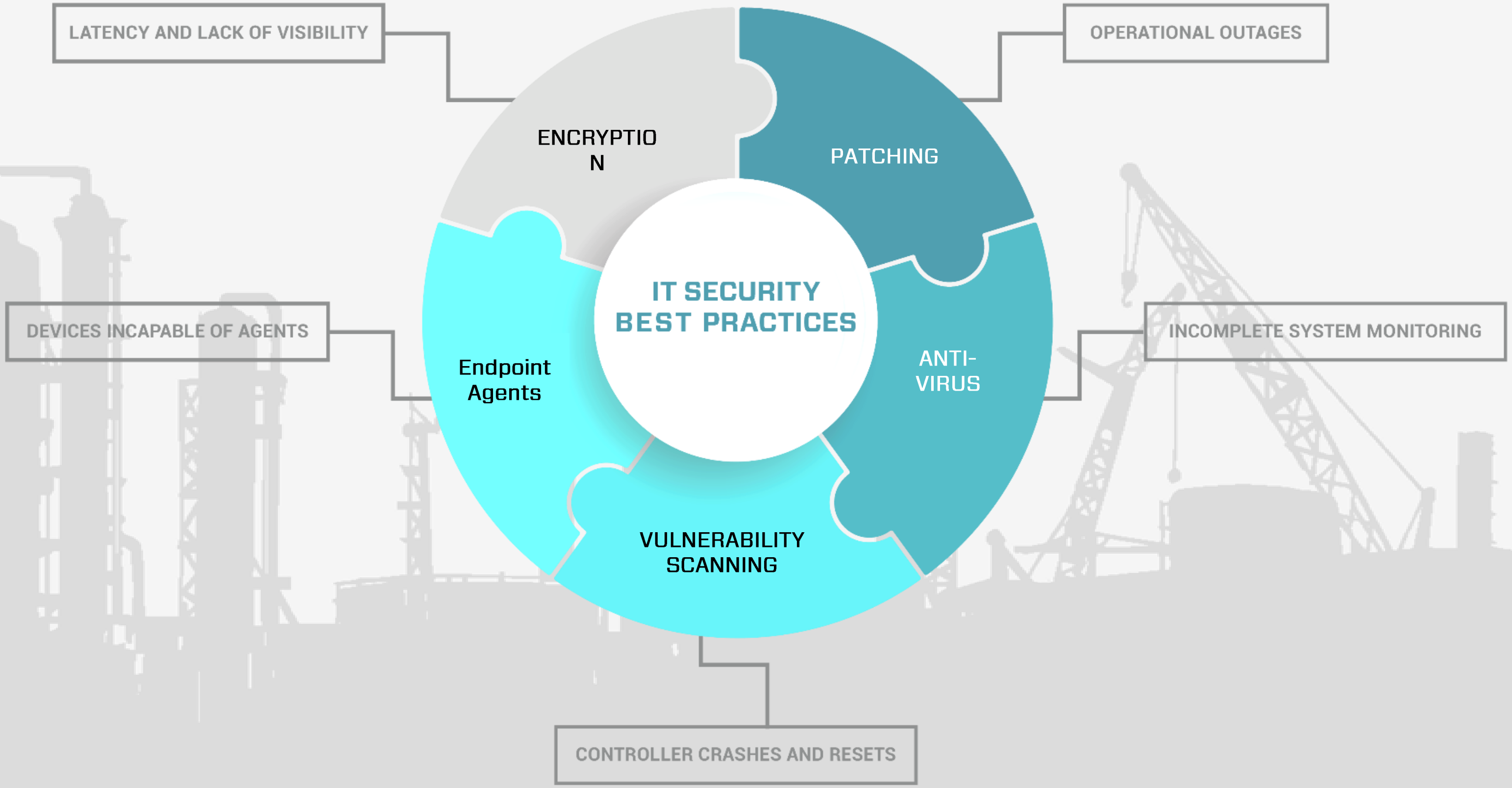
OT vs. IT

Specific impacts to security controls, incident response, and risk evaluation within OT environments

Culture

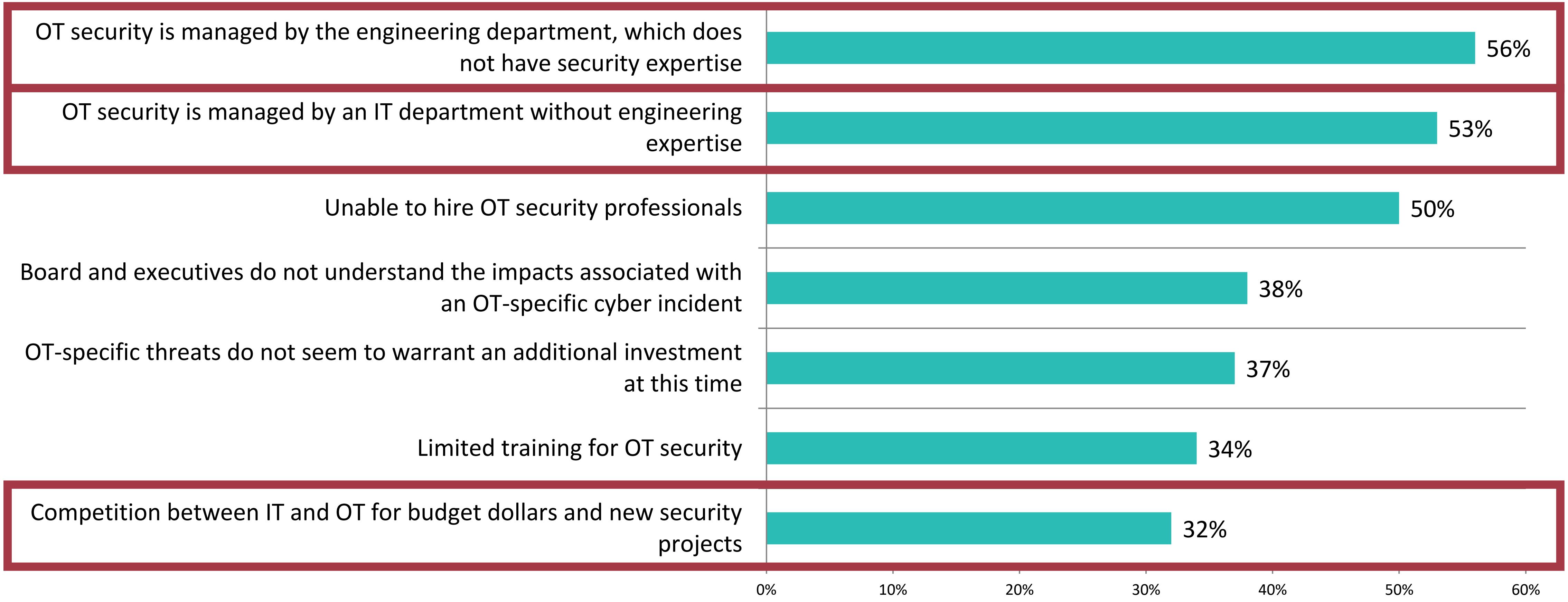
Increased focus on safety and reliability as a “wrapper” for security

Not all security controls are equal



LATENCY AND LACK OF VISIBILITY
OPERATIONAL OUTAGES
ENCRYPTIO N
PATCHING
IT SECURITY BEST PRACTICES
DEVICES INCAPABLE OF AGENTS
Endpoint Agents
ANTI- VIRUS
INCOMPLETE SYSTEM MONITORING
VULNERABILITY SCANNING
CONTROLLER CRASHES AND RESETS

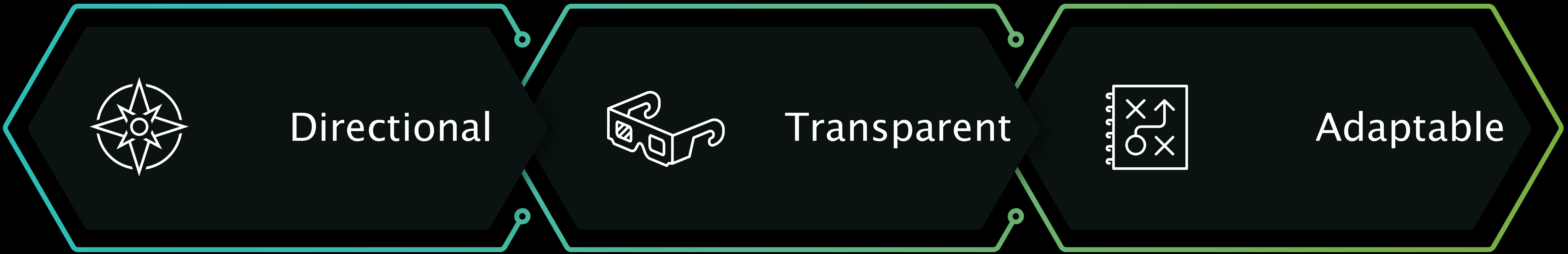
Insights to Challenges



Source: https://www.dragos.com/resource/2021-state-of-industrial-cybersecurity-ponemon/

Using Roadmaps

A deceptively simple solution



Directional

Transparent

Adaptable

Roadmaps help:

- Align business objectives to cyber risk
- Prioritize projects and programmatic improvements

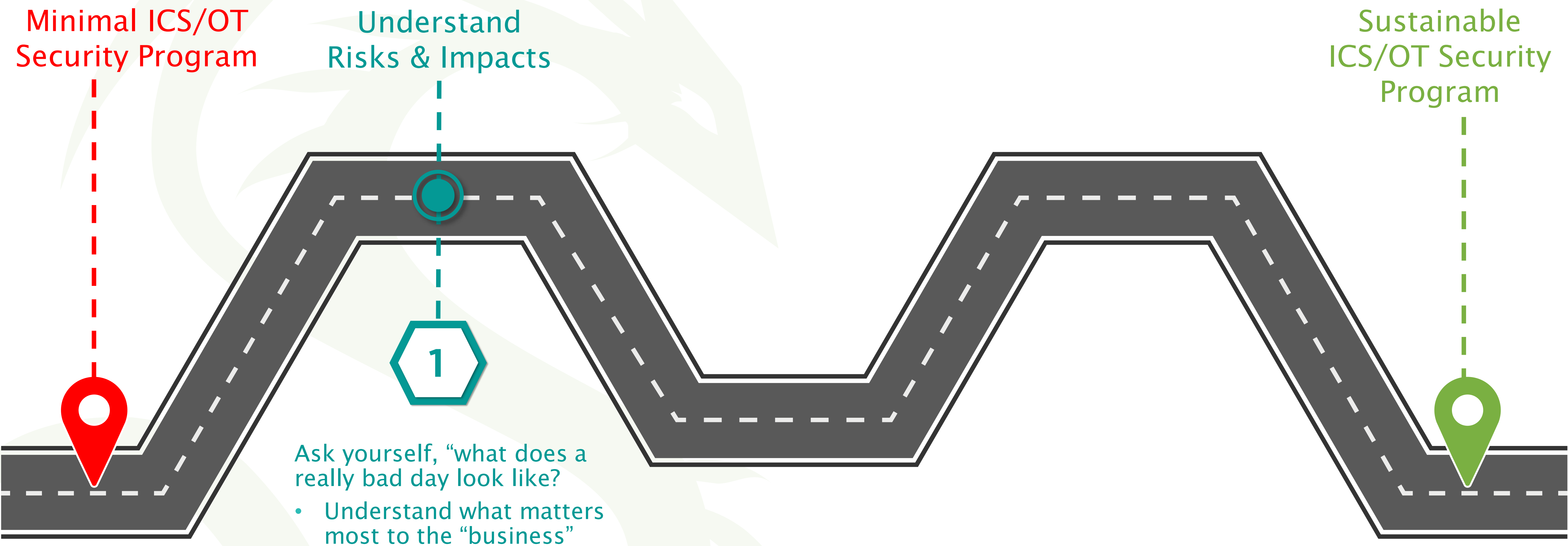
When broadly shared, they also:

- Provide insights into resourcing needs
- Can be tied to threat trends and incidents

Roadmaps **are not**:

- Auditable standards
- Written in stone
- Replacements for cyber risk governance models

How do we get there?


Minimal ICS/OT Security Program
Understand Risks & Impacts
1
Sustainable ICS/OT Security Program

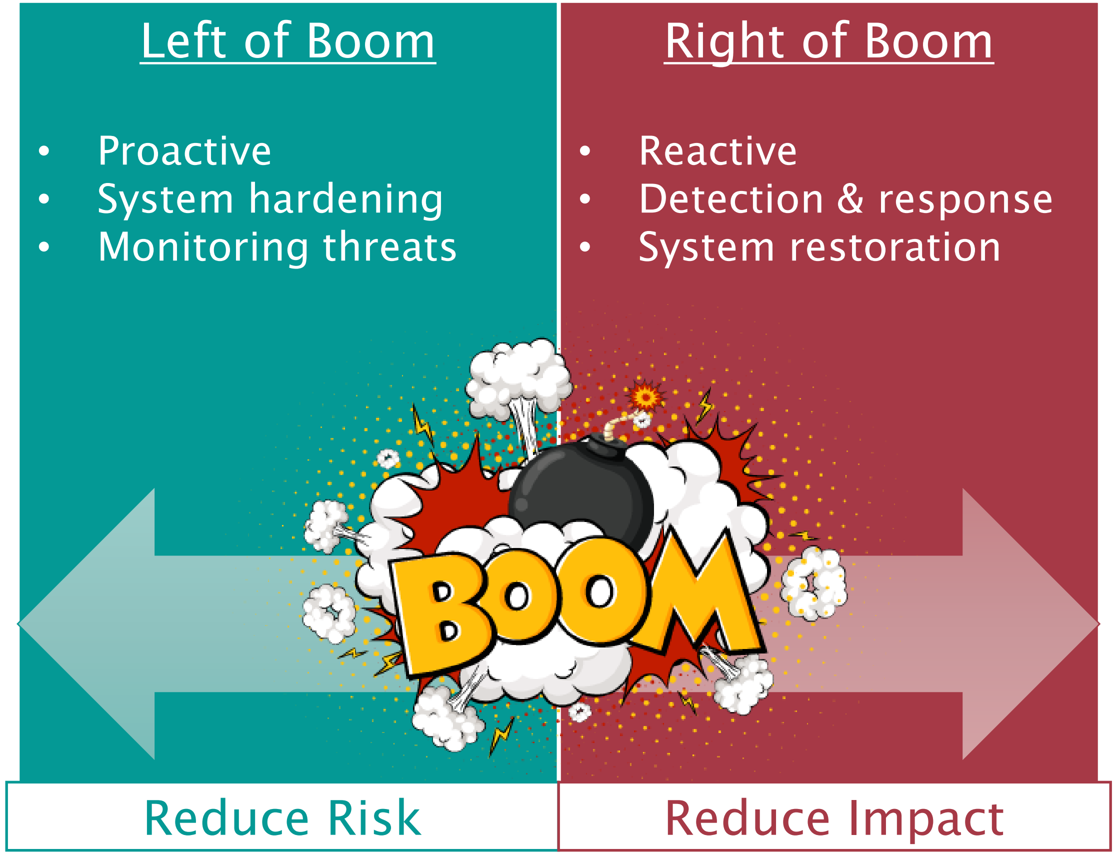
Ask yourself, "what does a really bad day look like?

- Understand what matters most to the "business"
- Evaluate potential impacts

Understand Risks & Impacts

1

Bad days and crown jewels



Left of Boom

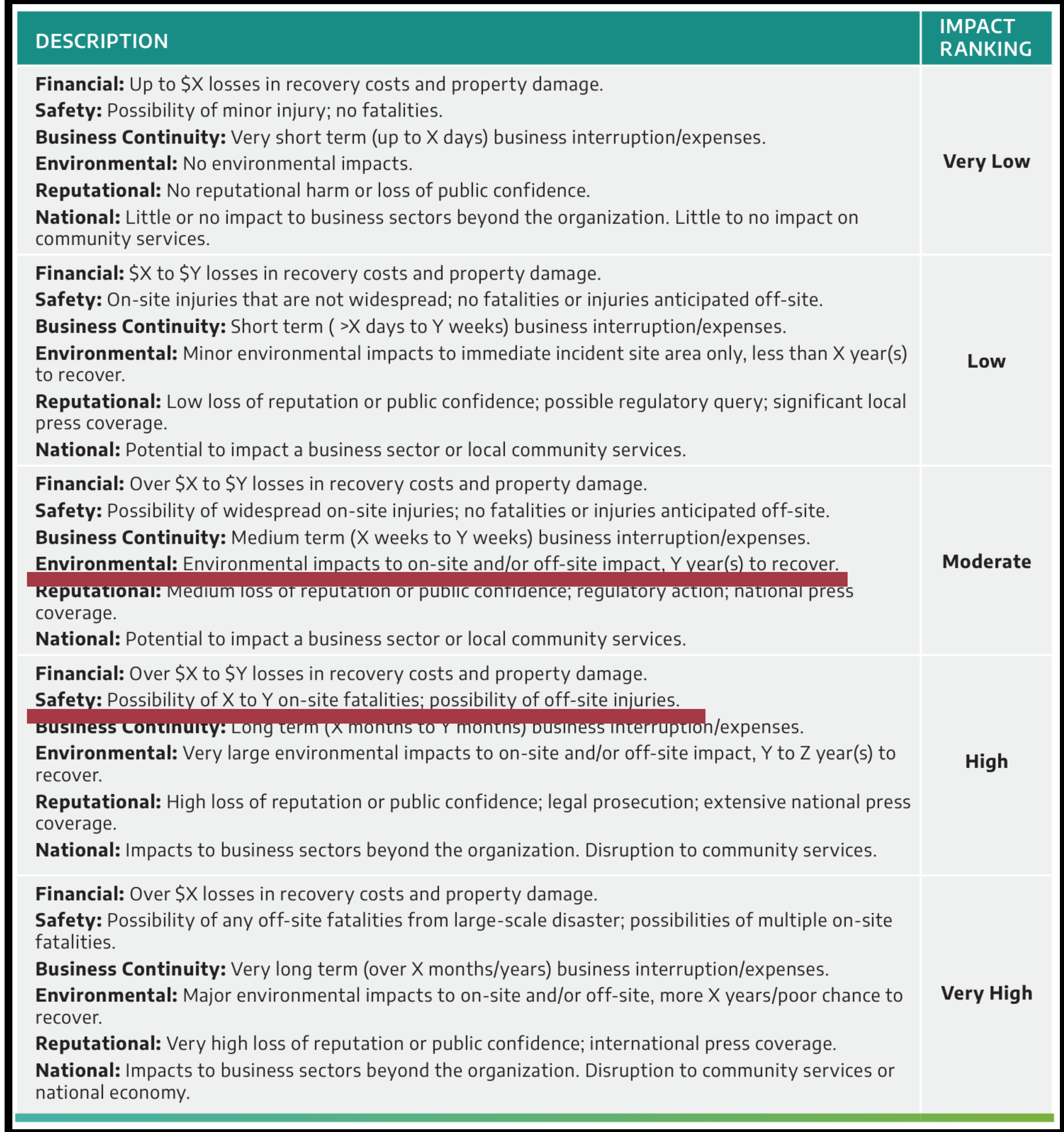
- Proactive
- System hardening
- Monitoring threats

Right of Boom

- Reactive
- Detection & response
- System restoration

Reduce Risk

Reduce Impact



DESCRIPTION	IMPACT RANKING
Financial: Up to $X losses in recovery costs and property damage. **Safety:** Possibility of minor injury; no fatalities. **Business Continuity:** Very short term (up to X days) business interruption/expenses. **Environmental:** No environmental impacts. **Reputational:** No reputational harm or loss of public confidence. **National:** Little or no impact to business sectors beyond the organization. Little to no impact on community services.	Very Low
Financial: $X to $Y losses in recovery costs and property damage. **Safety:** On-site injuries that are not widespread; no fatalities or injuries anticipated off-site. **Business Continuity:** Short term (>X days to Y weeks) business interruption/expenses. **Environmental:** Minor environmental impacts to immediate incident site area only, less than X year(s) to recover. **Reputational:** Low loss of reputation or public confidence; possible regulatory query; significant local press coverage. **National:** Potential to impact a business sector or local community services.	Low
Financial: Over $X to $Y losses in recovery costs and property damage. **Safety:** Possibility of widespread on-site injuries; no fatalities or injuries anticipated off-site. **Business Continuity:** Medium term (X weeks to Y weeks) business interruption/expenses. **Environmental:** Environmental impacts to on-site and/or off-site impact, Y year(s) to recover. **Reputational:** Medium loss of reputation or public confidence; regulatory action; national press coverage. **National:** Potential to impact a business sector or local community services.	Moderate
Financial: Over $X to $Y losses in recovery costs and property damage. **Safety:** Possibility of X to Y on-site fatalities; possibility of off-site injuries. **Business Continuity:** Long term (X months to Y months) business interruption/expenses. **Environmental:** Very large environmental impacts to on-site and/or off-site impact, Y to Z year(s) to recover. **Reputational:** High loss of reputation or public confidence; legal prosecution; extensive national press coverage. **National:** Impacts to business sectors beyond the organization. Disruption to community services.	High
Financial: Over $X losses in recovery costs and property damage. **Safety:** Possibility of any off-site fatalities from large-scale disaster; possibilities of multiple on-site fatalities. **Business Continuity:** Very long term (over X months/years) business interruption/expenses. **Environmental:** Major environmental impacts to on-site and/or off-site, more X years/poor chance to recover. **Reputational:** Very high loss of reputation or public confidence; international press coverage. **National:** Impacts to business sectors beyond the organization. Disruption to community services or national economy.	Very High

Source: https://www.dragos.com/resource/industrial-cyber-risk-management/

Historic

- Real events based on data from your organization, industry, or peers
- No explanation needed for plausibility
- Can be evaluated with minor internal information requests

VS

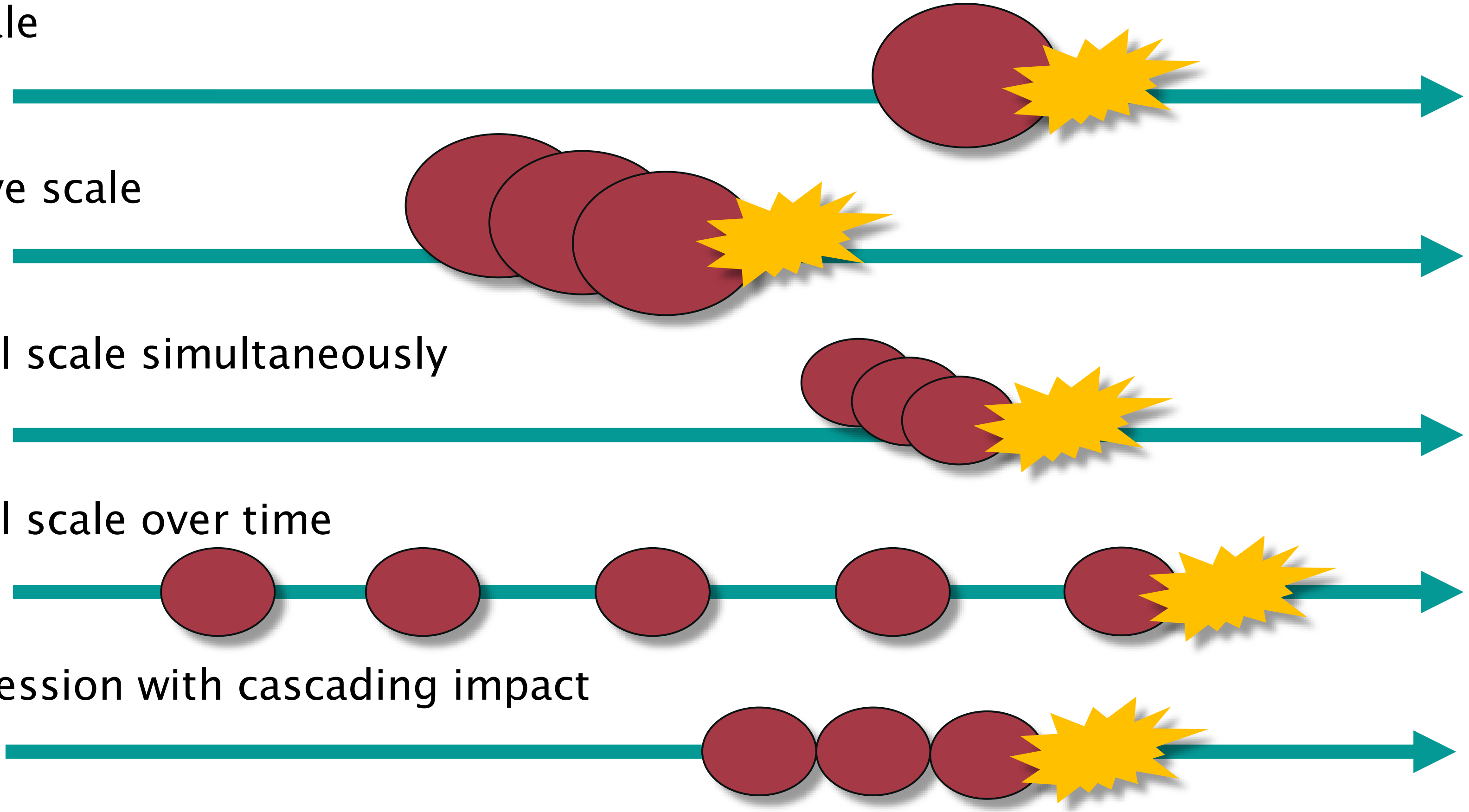
Hypothetical

- Hypothetical, yet plausible, events that may reasonably occur with a set impact
- Plausibility requires business unit input
- Requires judgement, trained resources, and understanding of the business unit

An industrial cyber risk management approach for OT must include both.

Scenario Scale Considerations

Choose your own adventure



One scenario, massive scale

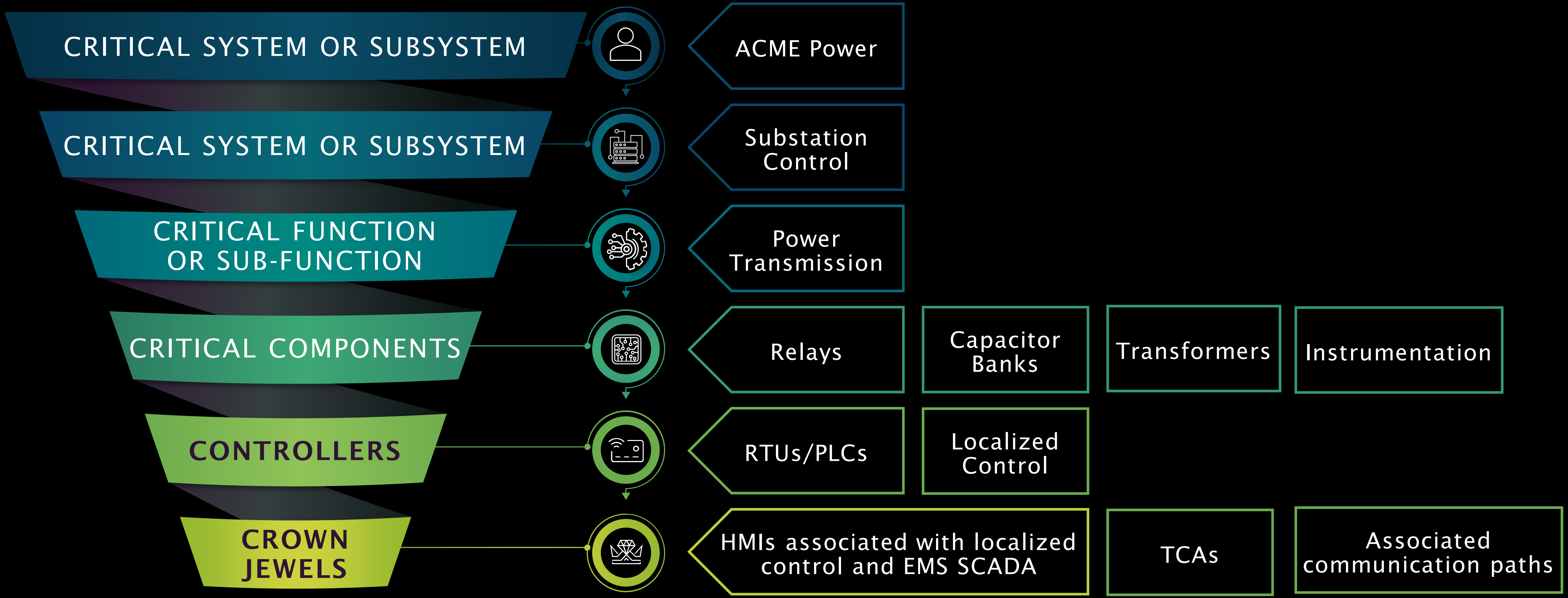
Multiple scenarios, massive scale

Multiple scenarios at small scale simultaneously

Multiple scenarios at small scale over time

Multiple scenarios in succession with cascading impact

Related "Crown Jewels"



CRITICAL SYSTEM OR SUBSYSTEM — ACME Power

CRITICAL SYSTEM OR SUBSYSTEM — Substation Control

CRITICAL FUNCTION OR SUB-FUNCTION — Power Transmission

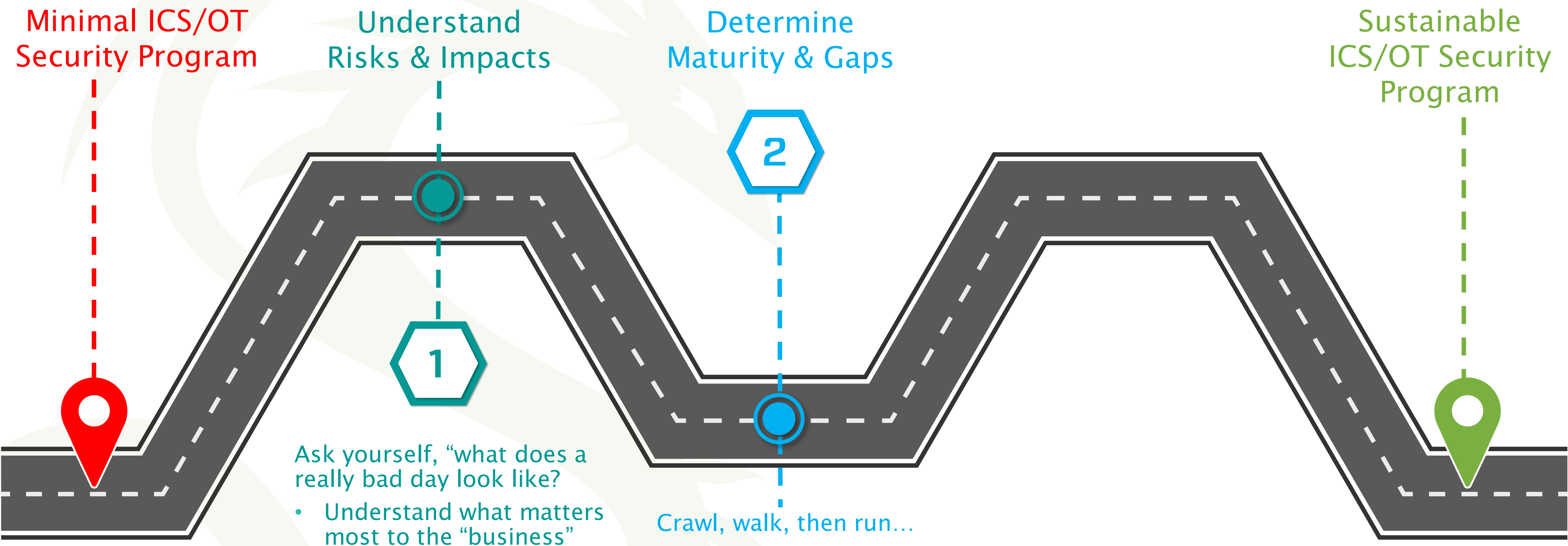
CRITICAL COMPONENTS — Relays; Capacitor Banks; Transformers; Instrumentation

CONTROLLERS — RTUs/PLCs; Localized Control

CROWN JEWELS — HMIs associated with localized control and EMS SCADA; TCAs; Associated communication paths

Source: https://www.dragos.com/blog/industry-news/combating-cyber-attacks-with-consequence-driven-ics-cybersecurity/

How do we get there?



Minimal ICS/OT Security Program

Understand Risks & Impacts

Determine Maturity & Gaps

Sustainable ICS/OT Security Program

Ask yourself, “what does a really bad day look like?

- Understand what matters most to the “business”
- Evaluate potential impacts

Crawl, walk, then run…

- Be honest about your capabilities
- Understand your current and future states

What do we mean by “maturity?”

First, you need to
CRAWL

- Initial defenses may be resource-constrained
- No documentation, no lessons learned
- Loss of “lotto winners” could cripple the program

Then you can
WALK

- Moving beyond ”oral history” to written law
- Partnered with multiple stakeholders
- Resources are less scarce

Finally, let’s
RUN

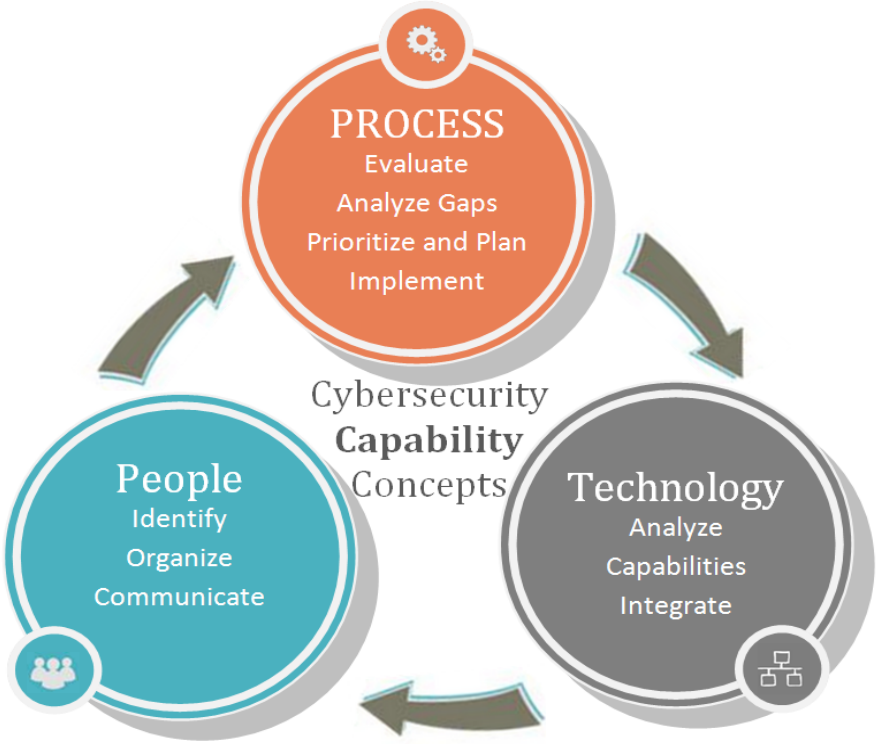
- People are trained, ready, and exercised
- Executives are active participants in ICS security
- Capabilities are “double-checked” and reviewed

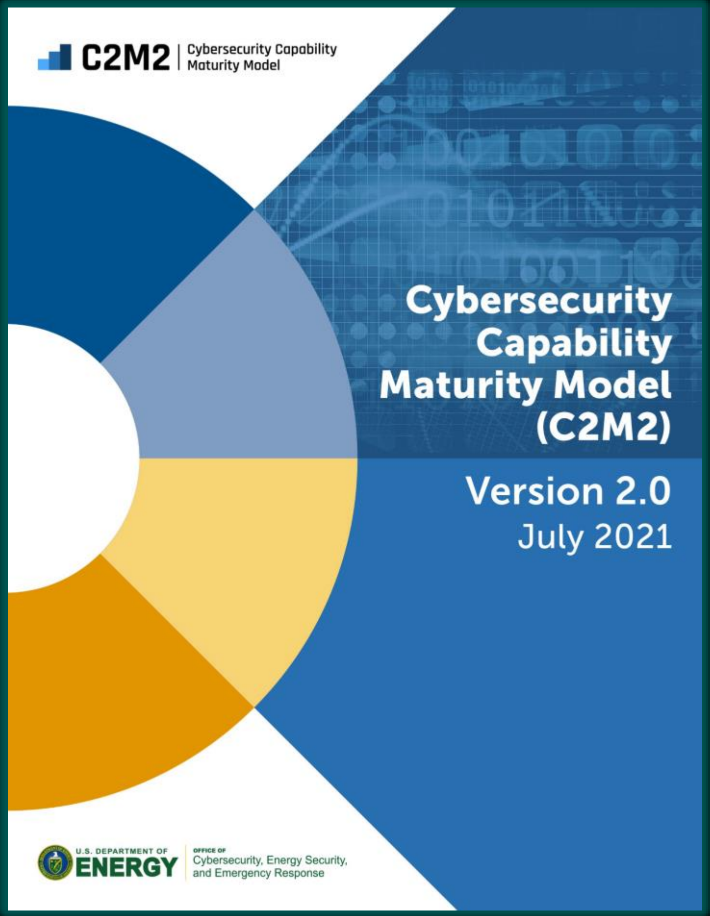
These various “Maturity Idicator Levels” (MILs) can *indicate* potential areas for growth.

Determine Maturity & Gaps

2

Evaluating capabilities




C2M2 | Cybersecurity Capability Maturity Model

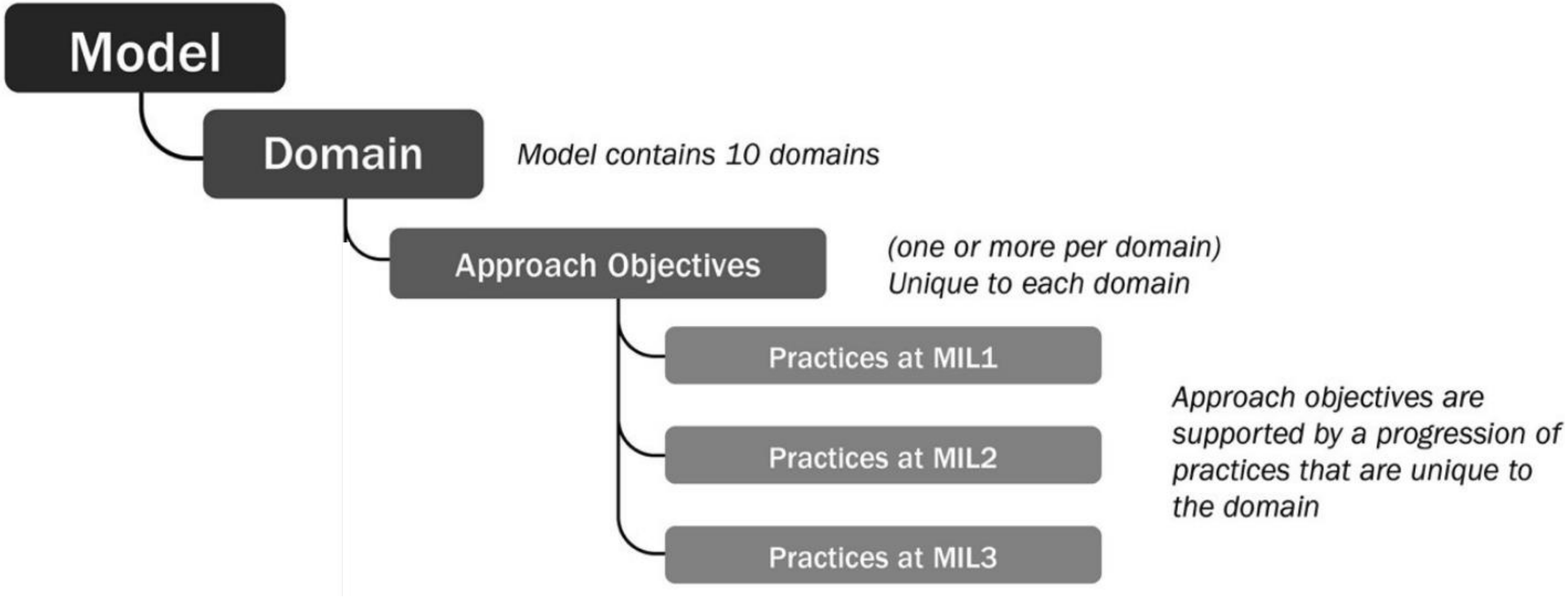
Cybersecurity Capability Maturity Model (C2M2)

Version 2.0
July 2021

U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

Source: https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

Organization of a Domain

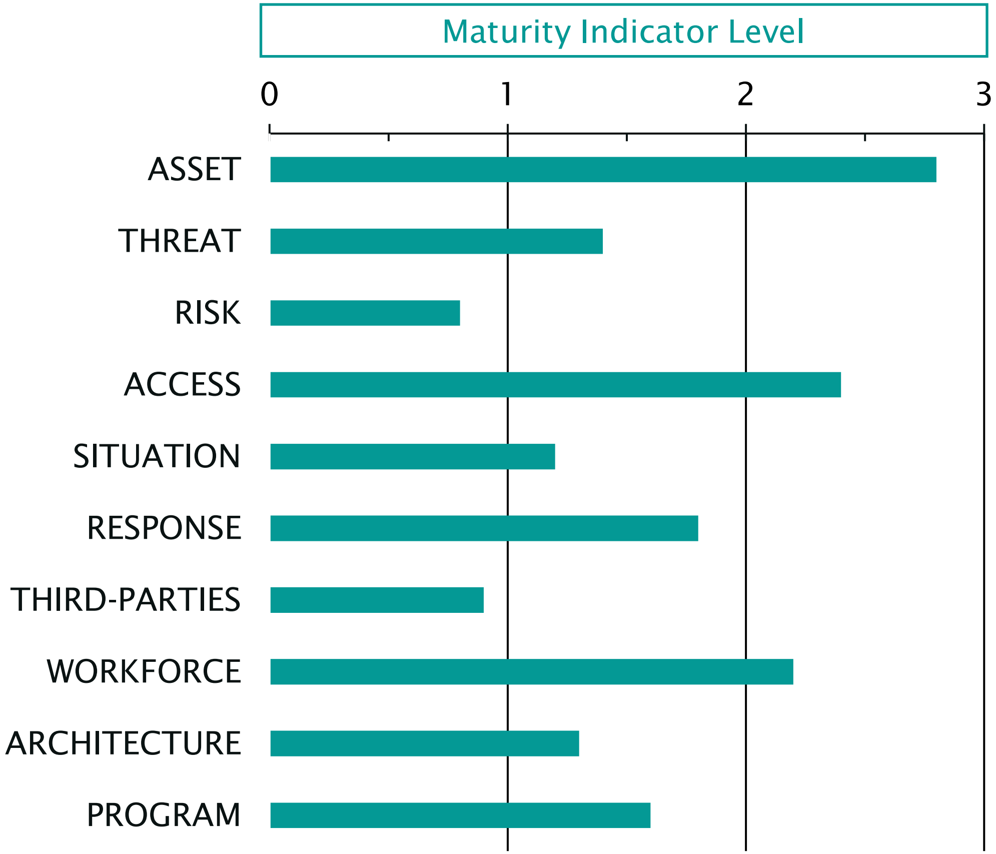


Model contains 10 domains

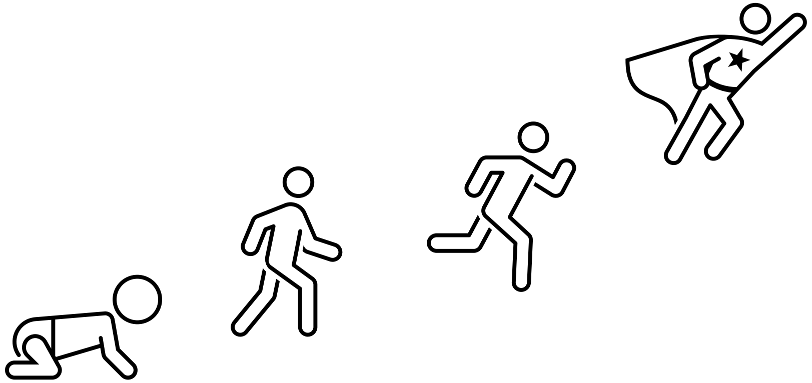
(one or more per domain)
Unique to each domain

Approach objectives are supported by a progression of practices that are unique to the domain

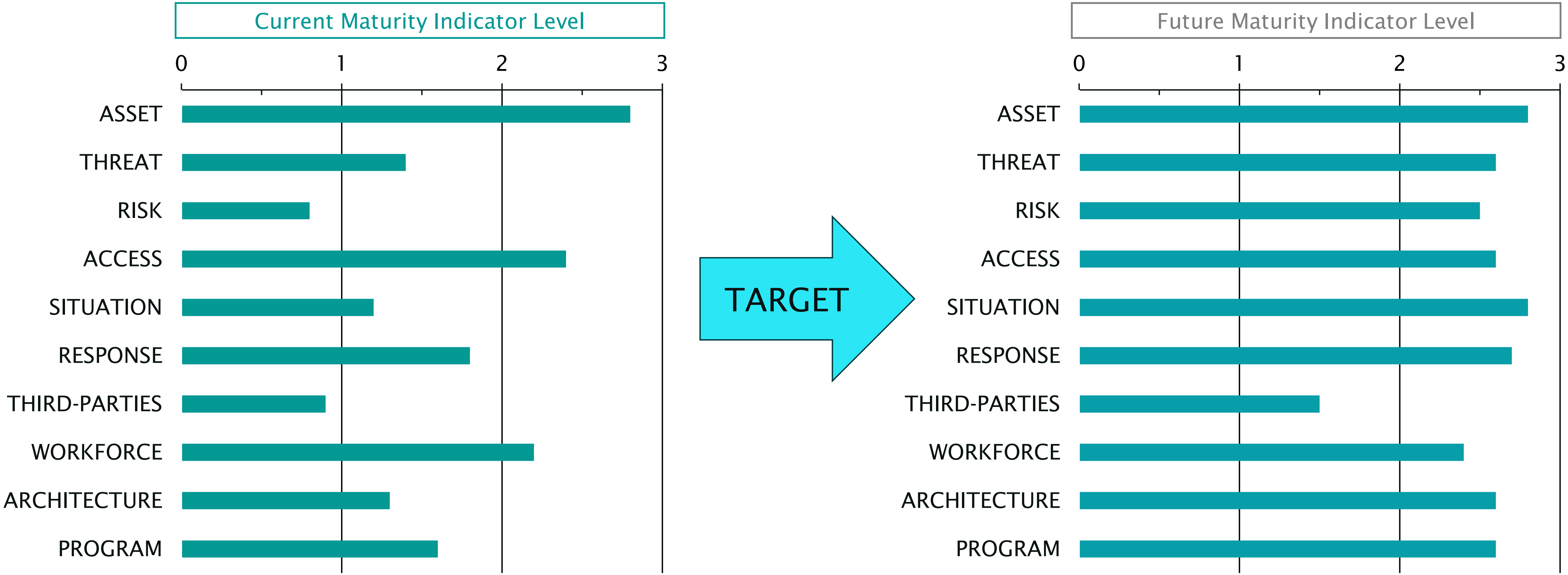
Current and Future States



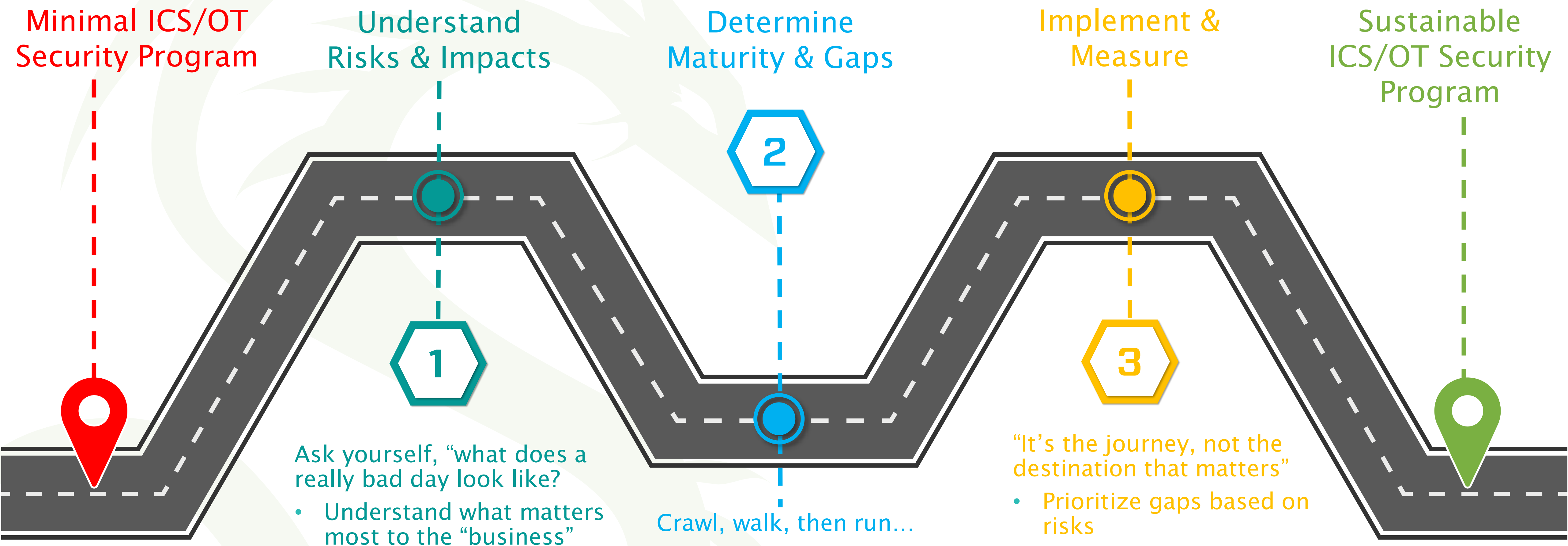
Maturity models can help establish “where you are” in your journey, based on the resources you have, applied to a crawl-walk-run approach.



Current and Future States



How do we get there?



Minimal ICS/OT Security Program

Understand Risks & Impacts

Determine Maturity & Gaps

Implement & Measure

Sustainable ICS/OT Security Program

Ask yourself, “what does a really bad day look like?

- Understand what matters most to the “business”
- Evaluate potential impacts

Crawl, walk, then run…

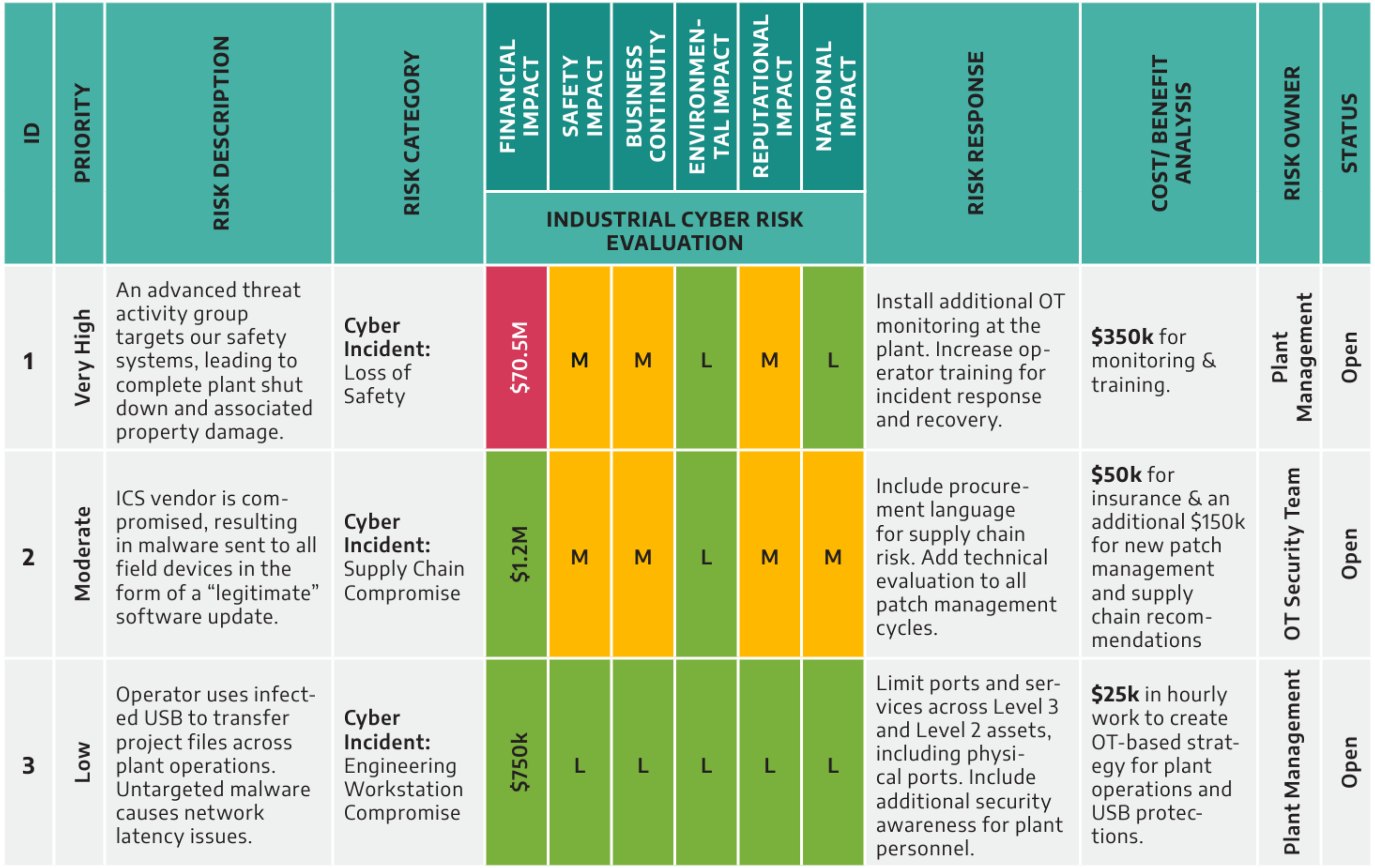
- Be honest about your capabilities
- Understand your current and future states

“It’s the journey, not the destination that matters”

- Prioritize gaps based on risks
- Create methods for consistent measurement to note success

Implement & Measure

Practical use of risk registers



ID	PRIORITY	RISK DESCRIPTION	RISK CATEGORY	FINANCIAL IMPACT	SAFETY IMPACT	BUSINESS CONTINUITY	ENVIRONMENTAL IMPACT	REPUTATIONAL IMPACT	NATIONAL IMPACT	RISK RESPONSE	COST/ BENEFIT ANALYSIS	RISK OWNER	STATUS
				INDUSTRIAL CYBER RISK EVALUATION									
1	Very High	An advanced threat activity group targets our safety systems, leading to complete plant shut down and associated property damage.	**Cyber Incident:** Loss of Safety	$70.5M	M	M	L	M	L	Install additional OT monitoring at the plant. Increase operator training for incident response and recovery.	**$350k** for monitoring & training.	Plant Management	Open
2	Moderate	ICS vendor is compromised, resulting in malware sent to all field devices in the form of a "legitimate" software update.	**Cyber Incident:** Supply Chain Compromise	$1.2M	M	M	L	M	M	Include procurement language for supply chain risk. Add technical evaluation to all patch management cycles.	**$50k** for insurance & an additional $150k for new patch management and supply chain recommendations	OT Security Team	Open
3	Low	Operator uses infected USB to transfer project files across plant operations. Untargeted malware causes network latency issues.	**Cyber Incident:** Engineering Workstation Compromise	$750k	L	L	L	L	L	Limit ports and services across Level 3 and Level 2 assets, including physical ports. Include additional security awareness for plant personnel.	**$25k** in hourly work to create OT-based strategy for plant operations and USB protections.	Plant Management	Open

A risk register is:

- One stop shop for high-level risk discussions
- A management and tracking tool

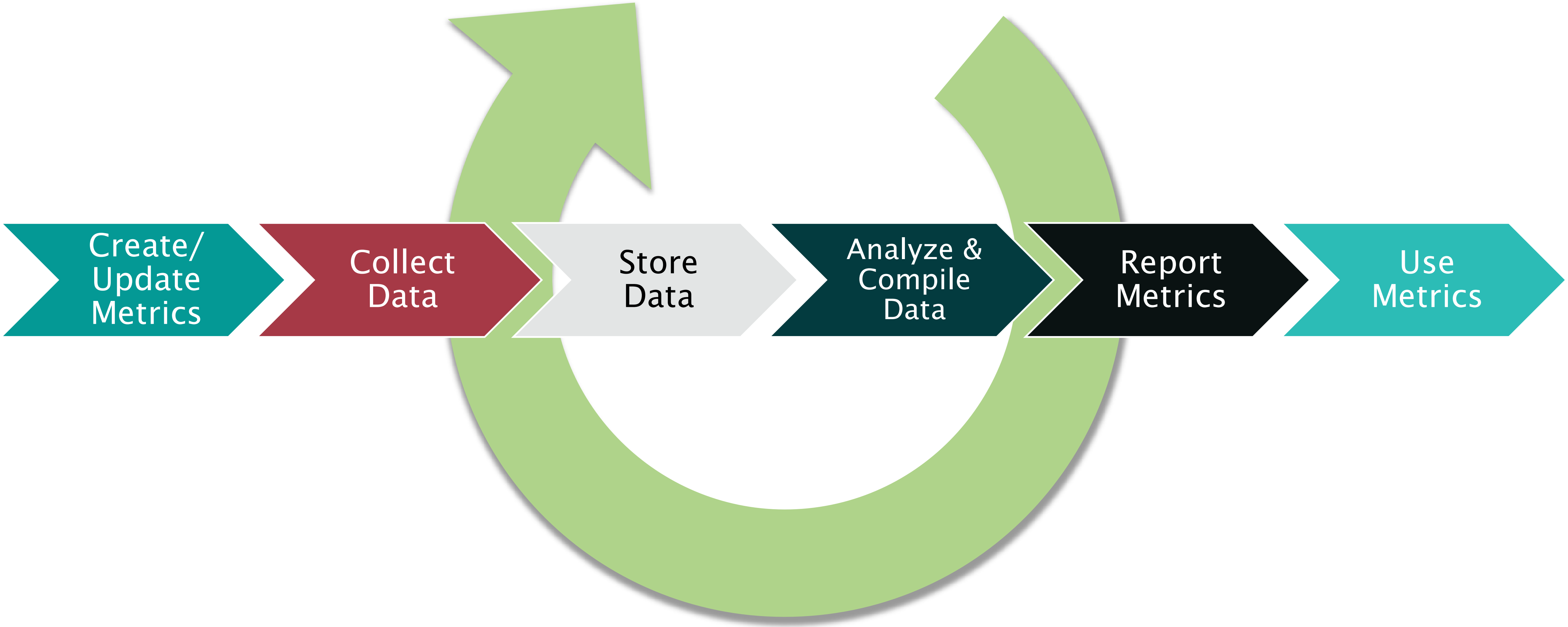
A risk register is not:

- Static: it must be used to be useful
- Magic: risks still need to be managed!

DRAGOS

Source: https://www.dragos.com/OTcyberrisk

Metrics and more indicators!



Create/ Update Metrics

Collect Data

Store Data

Analyze & Compile Data

Report Metrics

Use Metrics

A quick word on “measuring what matters”

Not all measurements are equal

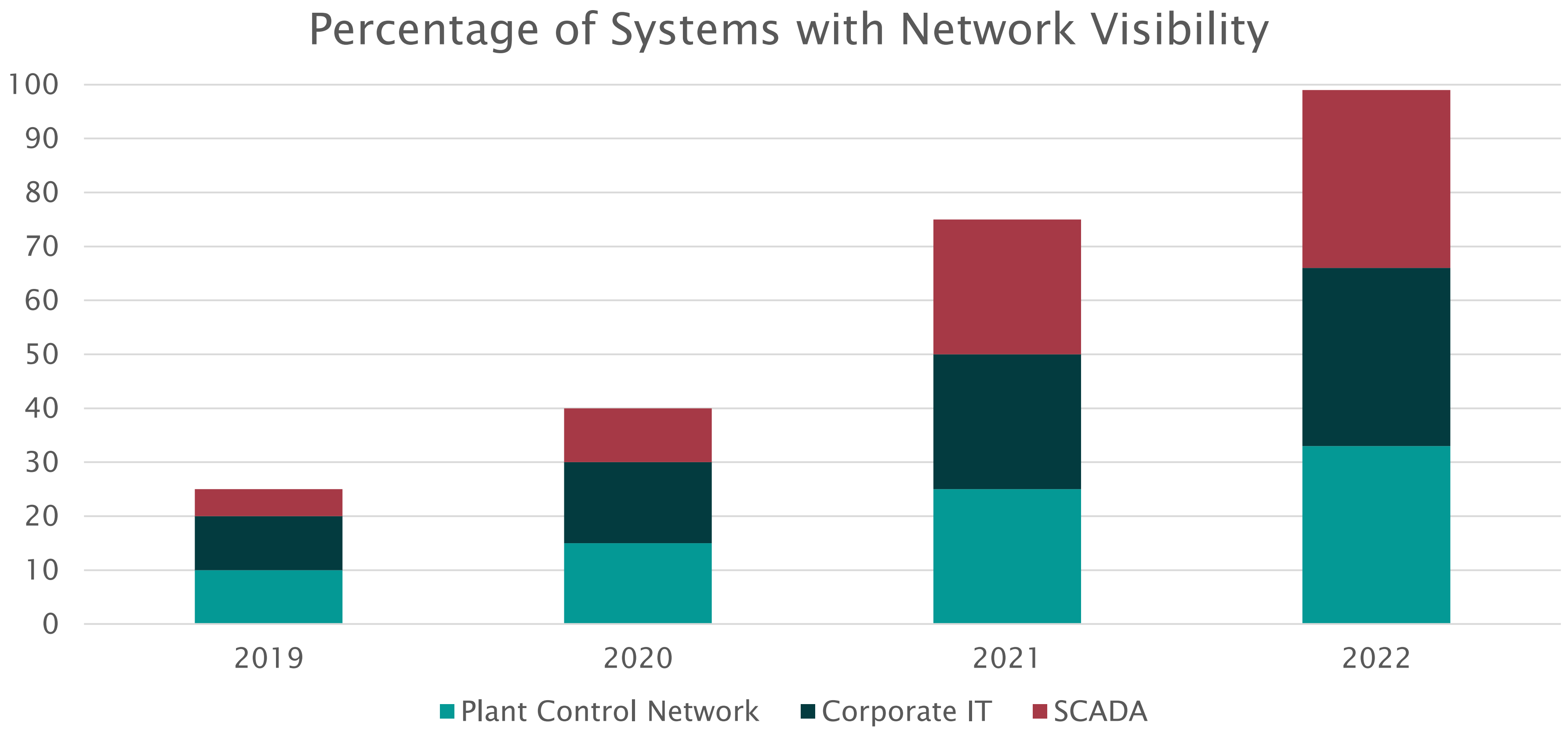
- State goals and benefits
- Identify data sources (both automated and manual)
- Understand how goals/benefits relate to data
- Create a series of metrics to support

Goal	KPI	Benefit	Data Needed
Decrease potential down time from ICS cyber incident	Mean-Time-to-Fix (MTTF)	Demonstrates IR team’s effectiveness	Hours spent on incidents
	Incidents Requiring Manual Clean-up	Highlights trend of IR requiring manual effort	IR tickets and total number of incidents with malware
	Number of ICS security skills per employee	Track and improve IR team capabilities	HR and training information

Source: https://sans.org/ics418

Too advanced?

Then pick what works for you. The right first metric could be as simple as:



PROTECTING THE CROWN JEWELS

“PROTECTION IS IDEAL, DETECTION IS A MUST”

Real-life Application

Manufacturing Use Case

Initial discussion

“How good are we doing?” led to an in-depth discussion on crown jewels and the architecture within the relevant systems.

Unsurprisingly– issues were found.

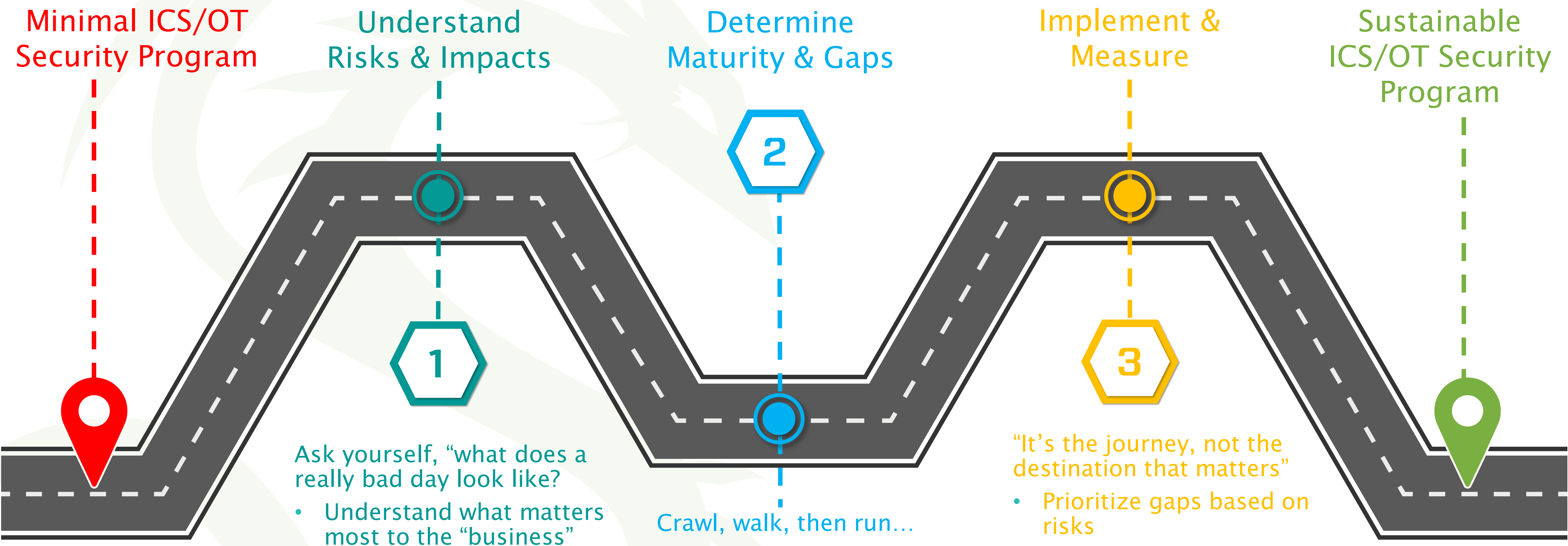
Quick Wins

Immediate remediation with both “low hanging fruit” and high severity issues across incident response, network visibility, and system hardening.

Scorecards and Success

Only one year later, established a more robust program linking projects to maturity levels, board and executives were more aligned to OT and IT cyber risk relationships.

How do we get there?



Minimal ICS/OT Security Program

Understand Risks & Impacts

Determine Maturity & Gaps

Implement & Measure

Sustainable ICS/OT Security Program

Ask yourself, “what does a really bad day look like?

- Understand what matters most to the “business”
- Evaluate potential impacts

Crawl, walk, then run…

- Be honest about your capabilities
- Understand your current and future states

“It’s the journey, not the destination that matters”

- Prioritize gaps based on risks
- Create methods for consistent measurement to note success

Questions?

Jason D. Christopher
Director of Cyber Risk
jdchristopher@dragos.com