Best Practices:
Cybersecurity Tabletop Exercises (TTX) Aligned with Organization's Maturity Level + Auto Tabletop Demo

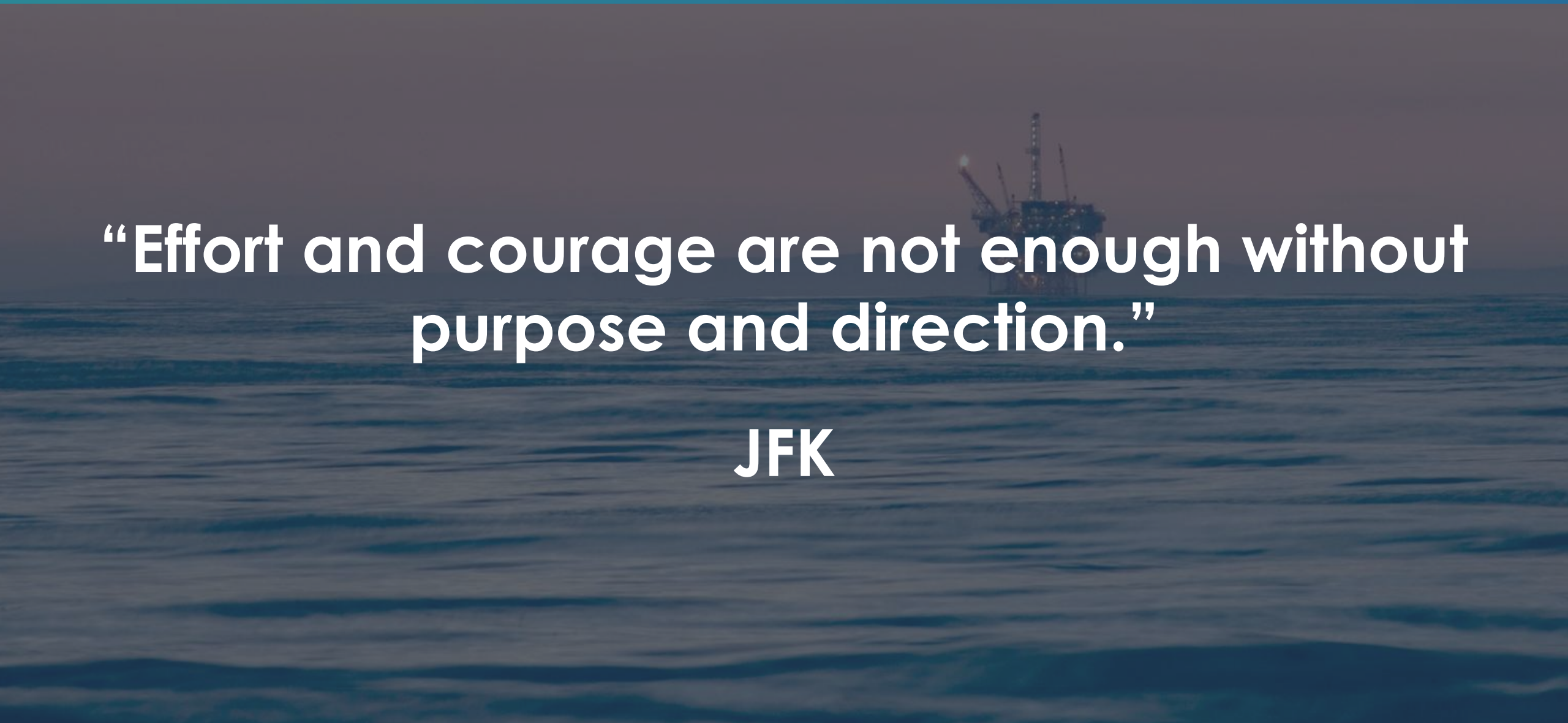
Shaun Six,
President, UTSI

Clint Bodungen,
Founder, ThreatGEN

6/12/25

utsi.com threatgen.com

INTRODUCTION



"Effort and courage are not enough without purpose and direction."

JFK

CYBERSECURITY CHALLENGES FOR CRITICAL OPERATIONS

In today's interconnected world, safeguarding your critical operations from cyber threats is more important than ever.

73% of organizations experienced intrusions that impacted OT systems in 2024, up from 49% in 2023.

46% of intrusions occur due to negligent insiders with trusted access.

More than **34%** of global (ICS) computers saw a malicious attack in 2023.

40% of OT/ICS asset base is outdated posing significant cybersecurity risk.

Critical infrastructure knowledge gap is **5:1** replacement of workers.

33% of engineering roles go unfulfilled in the U.S.

TODAY'S TOPICS

- ✓ Introductions
- ✓ Cybersecurity Maturity Model Frameworks
- ✓ Benefits of Maturity Assessments
- ✓ Sample Maturity Model Tiers, Roadmap and Scorecards
- ✓ Live Demo of ThreatGEN's AutoTableTop tool
- ✓ Summary of Best Practices
- ✓ Q & A

SHAUN SIX, PRESIDENT, UTSI

Experience:

20 years in O&G, IT/OT Project Management
- First TTX and Maturity Assessment at Devon Energy 2007
  - BCP, ERP, IRP

BHP ICS – Communications Unit (Logistics)
- Cyber Attacks via malware, social engineering, "sneakerware"
- ICS Response to rig fire, well blowout, county-wide comms outage

Maturity Assessment as Facilitator
- AI/Data Science – 2016 (ACN) "AI Hierarchy of Needs"
- PMO – (JLT)
- IM / Doc Control / EDMS (RedEye)
- OT Cybersecurity (UTSI) - Water/Wastewater, Upstream, Midstream, Downstream O&G
- Working on "Digital Twin" MA for a client and vendor

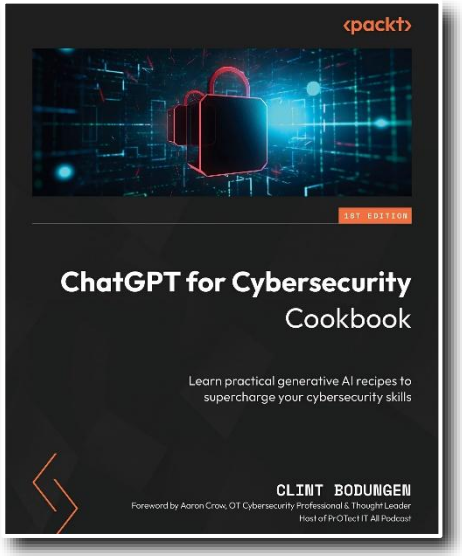
Industry Threats:

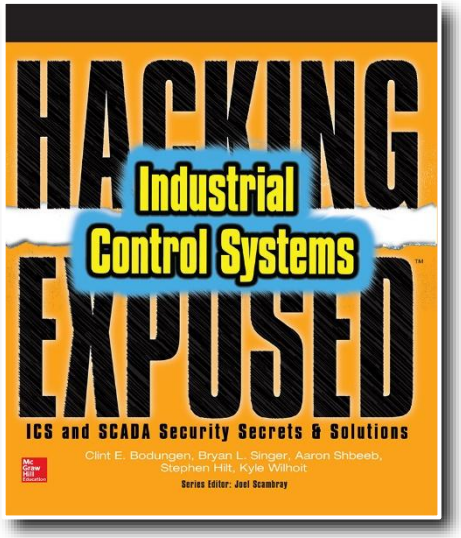
1. Lacked OT focused cybersecurity frameworks and concepts, and the inclusion / feedback from maturity assessments.
2. Completed Maturity Assessments were often used as compliance rather than being leveraged to build a roadmap or plan.
3. "Current state" assessments and "as-is" capabilities weren't utilized, making them unrealistic and leaving organizations unprepared for real-world scenarios.

CLINT BODUNGEN, FOUNDER, THREATGEN

Experience:

- Director, Cybersecurity Innovation – Morgan Franklin Cyber
- Founder – ThreatGEN
- USAF veteran with 30 years in cybersecurity (25 in industrial cybersecurity)
- Worked with many of the world's largest energy companies and top cybersecurity firms
- Principle author of "Hacking Exposed: Industrial Control Systems"
- Author of “ChatGPT for Cybersecurity Cookbook”
- Creator of “ThreatGEN® Red vs. Blue” and “AutoTableTop™”
- Published multiple technical papers and training courses on ICS/OT cybersecurity





MATURITY MODEL FRAMEWORKS

A **Cybersecurity Maturity Model (CMM)** is a structured framework that helps organizations assess and improve their cybersecurity capabilities over time. It provides a **step-by-step approach** to managing cybersecurity risks, ensuring that security measures evolve as threats and technologies change.

Key Aspects of a Cybersecurity Maturity

Levels of Maturity:

Typically includes stages that progress from an **ad-hoc or reactive approach** to a **fully optimized and proactive cybersecurity strategy**.

Assessment Tool:

Helps organizations **identify gaps** in their cybersecurity posture and prioritize improvements.

Continuous Improvement:

Encourages organizations to **regularly update** their security strategies to adapt to evolving threats.

Examples of Standardized Framework:

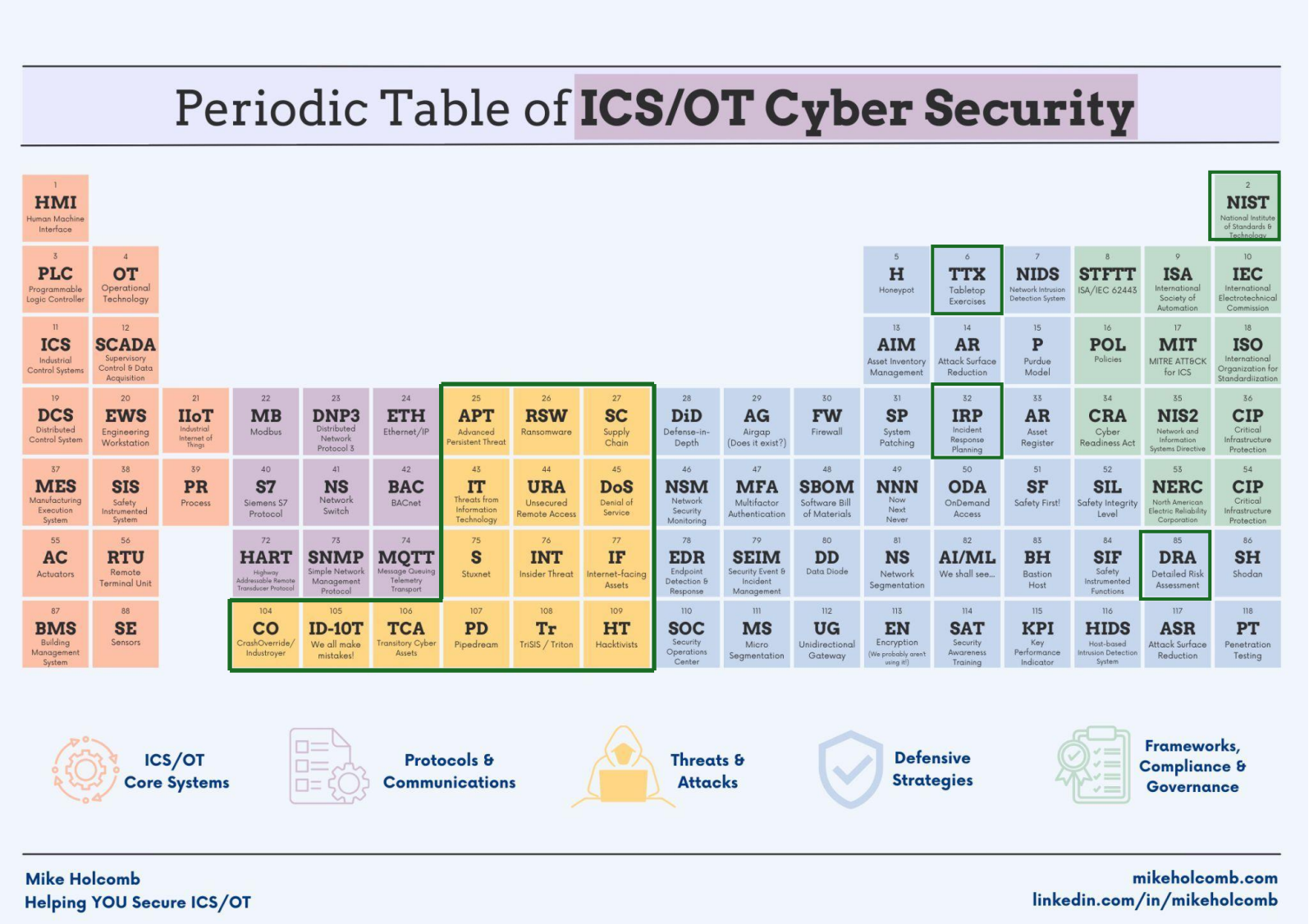
- C2M2 (Cybersecurity Capability Maturity Model)
- NIST Cybersecurity Framework (CSF)
- CMMC (Cybersecurity Maturity Model Certification)
- ISO 21827 Maturity Model

(not a comprehensive list)

Choosing the Right Framework:

- For U.S. Government/Defense Contractors : CMMC, NIST CSF
- For Enterprise Risk Management : ISO 27001, FAIR
- For IT Governance : COBIT, CMMI
- For Comprehensive Cybersecurity Strategy : NIST CSF, ISO 27001

MATURITY MODEL FRAMEWORKS



BENEFITS OF USING MATURITY ASSESSMENTS AS INPUTS TO TTX

Train and test against progress made since last TTX

Includes real capabilities and availability of technologies

Increases readiness of team and awareness of technological strengths and weaknesses

Provides feedback into the roadmap for confirmation of adoption, training, and validation of roadmap prioritization

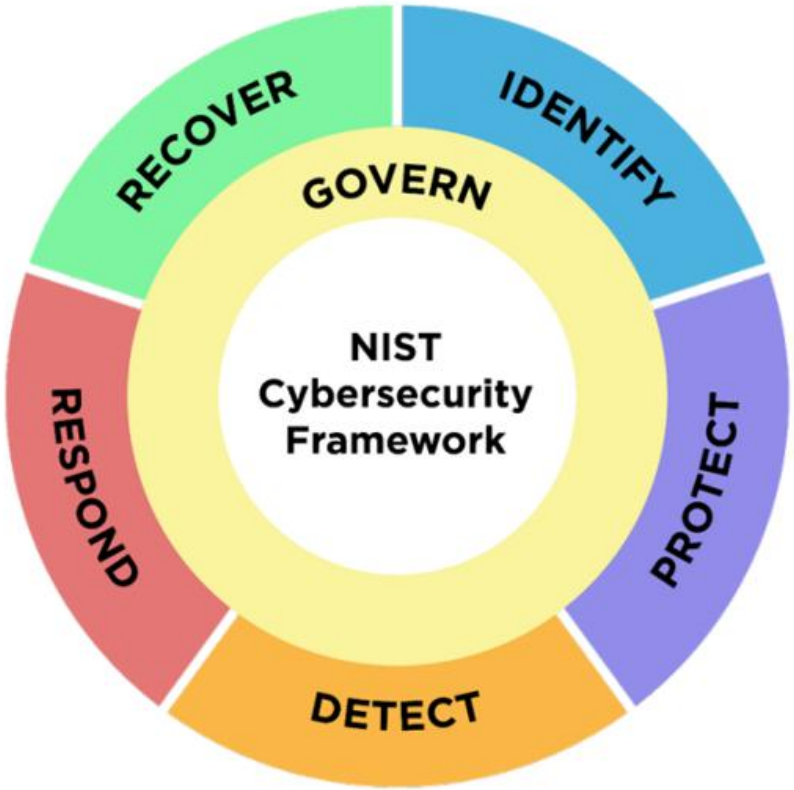
TTX feeds into your business continuity plans and incident response plans

MATURITY ASSESSMENT – GETTING STARTED

SELECT A FRAMEWORK	• Pick the right framework for your organization, discipline and industry • Tailor the framework to your organization • Work with partners and industry groups for feedback • Share your findings for inclusion and review with industry partners
INCLUDE ENTERPRISE AND OPERATIONS	• Assess where you are and decide where you'd like to be • Enterprise without operations will lack real world feedback • Operations without enterprise will risk buy-in and support
INCORPORATE THE FOLLOWING	• Inputs: Documents referenced and updated • Policies and Procedures • Incident Response Plan • Disaster Recovery Plan

NIST CSF 2.0

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Cybersecurity Supply Chain Risk Management	GV.SC
	Roles, Responsibilities, and Authorities	GV.RR
	Policies, Processes, and Procedures	GV.PO
	Oversight	GV.OV
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO



SAMPLE MATURITY MODEL FOR CSF 2.0

UTSI INTERNATIONAL

Function	Category	Tier 1 Partial	Tier 2 Risk Informed	Tier 3 Repeatable	Tier 4 Adaptive
Govern (GV)	Risk Management Strategy	No formal risk program	Basic risk assessments conducted	Standardized risk processes	Continuous monitoring & adaptation
	Cybersecurity Supply Chain Risk Mgmt	No supplier security checks	Some security requirements for vendor	Formal vendor risk assessments	Automated & real-time vendor risk monitoring
Identify (ID)	Asset Management	Untracked assets	Basic inventory, not regularly updated	Managed asset inventory	Continuous asset discovery & tracking
	Business Environment	No cybersecurity integration	Cybersecurity considered in some areas	Cybersecurity integrated into business strategy	Cybersecurity drives innovation and resilience
Protect (PR)	Access Control	No access controls or policies	Basic access controls, not consistently applied	Strong IAM policies	Adaptive, risk-based access management
Detect (DE)	Continuous Monitoring	No detection capabilities	Some logging, limited monitoring	SIEM in place	AI-driven threat detection, continuous analytics
Respond (RS)	Incident Management	No formal incident response plan	Basic response plan, inconsistently applied	Formal, tested incident response process	Automated response & mitigation capabilities
Recover (RC)	Incident Recovery Plan Execution	No disaster recovery planning	Basic recovery plan, not tested	Regularly tested disaster recovery plans	Adaptive, real-time recovery with automation

SAMPLE NIST CSF ASSESSMENT SCORE CARD

Function	Category	Tier Scoring
Govern (GV)	• Organizational Context • Risk Management Strategy • Cybersecurity Supply Chain Risk Management • Roles, Responsibilities & Authorities • Policies, Processes & Procedures • Oversight	2
Identify (ID)	• Asset Management • Risk Assessment • Improvement	3
Protect (PR)	• Identity Management, Authentication and Access Control • Awareness and Training • Data Security • Platform Security • Technology Infrastructure Resilience	2
Detect (DE)	• Continuous Monitoring • Adverse Event Analysis	2
Respond (RS)	• Incident Management • Incident Analysis • Incident Response Reporting and Communication • Incident Mitigation	1
Recover (RC)	• Incident Recovery Plan Execution • Incident Recovery Communication	1

NIST CSF MATURITY MODEL AND ROADMAP

UTSI INTERNATIONAL

NIST CSF 2.0 Maturity Model Rating

Govern	Identify	Protect	Detect	Respond	Recover
Tier 4 - Adaptable	Tier 4 - Adaptable	Tier 4 - Adaptable	Tier 4 - Adaptable	Tier 4 - Adaptable	Tier 4 - Adaptable
Tier 3 - Repeatable	Tier 3 - Repeatable	Tier 3 - Repeatable	Tier 3 - Repeatable	Tier 3 - Repeatable	Tier 3 - Repeatable
Tier 2 – Risk Informed	Tier 2 – Risk Informed	Tier 2 – Risk Informed	Tier 2 – Risk Informed	Tier 2 – Risk Informed	Tier 2 – Risk Informed
Tier 1 - Partial	Tier 1 - Partial	Tier 1 - Partial	Tier 1 - Partial	Tier 1 - Partial	Tier 1 - Partial

Govern

- Organizational Context
- Risk Management Strategy
- Cybersecurity Supply Chain Risk Management
- Roles, Responsibilities & Authorities
- Policies, Processes & Procedures
- Oversight

Identify

- Asset Management
- Risk Assessment
- Improvement

Protect

- Identity Management, Authentication and Access Control
- Awareness & Training
- Data Security
- Platform Security
- Technology Infrastructure Resilience

Detect

- Continuous Monitoring
- Adverse Event Analysis

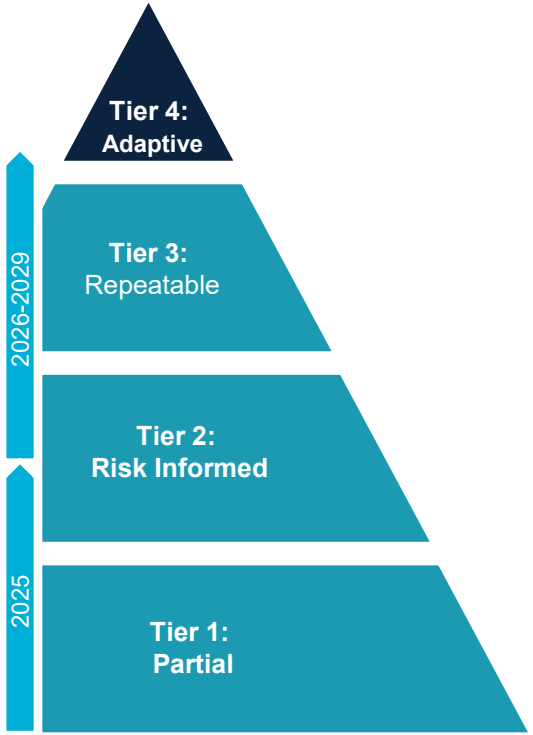
Respond

- Incident Management
- Incident Analysis
- Incident Response Reporting and Communication
- Incident Mitigation

Recover

- Incident Recovery Plan Execution
- Incident Recovery Communication

CYBERSECURITY MATURITY MODEL: TIER 3



Tier 3: Repeatable

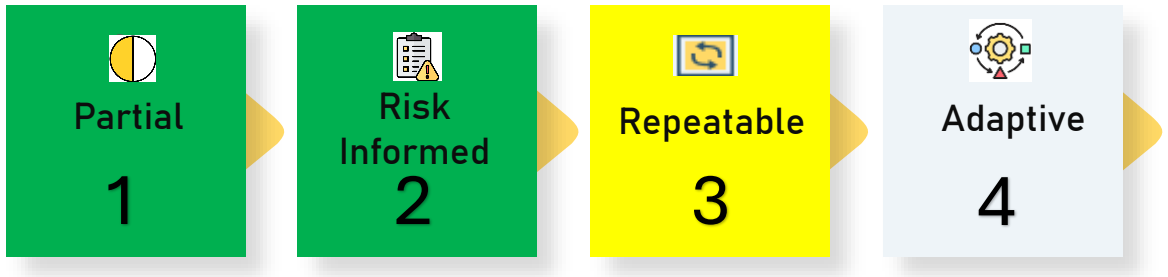
Definition: The organization has a structured, repeatable approach to cybersecurity risk management.

Characteristics:

- Documented and repeatable processes for managing cyber threats.
- Cybersecurity practices are regularly reviewed and updated.
- Well-defined cybersecurity requirements and goals.
- A skilled security team effectively handles cyber incidents.
- Active monitoring and assessment of cybersecurity posture.

Significance:

- Provides high protection against emerging threats.
- Considered the minimum level of cybersecurity maturity organizations should achieve.



BRIDGE BETWEEN ASSESSMENT AND TTX

Include inputs from the assessment to the tabletops:

- The tabletop assesses the capabilities at the current level and identify the gaps in skill, process, and tools.

- Once Maturity assessment is completed, develop a Table-Top Exercise that acknowledges the tools and capabilities at that level.

- The overall objective to maintain operation and remediate will be the same, however individual Tier based objectives will emerge.

SUMMARY OF TABLETOP BEST PRACTICES

UTSI INTERNATIONAL

- Understand how Tabletop exercises feed into your business continuity plans and trainings.
- Seek to identify gaps in your IR Plan and playbooks, iterate, and improve.
- Have a scribe/note taker (or record if you can)
- Pick scenarios that are relatable and real-world scenarios.
- Leverage AI. Ex: ThreatGen tool can schedule time to add in the personnel and their roles.
- Repetition is key. Once a year is not enough.
- You must have an incident commander who is in charge and makes decisions. During an incident is not decision by committee.
- Plan enough time for lessons learned and to go over the after-action report.
- Use a credible framework.
- Actively involve all stakeholders of the infrastructure being assessed.
- Exercises don't have to be multiple days (or even 1 entire day) to be effective.
- Have an IR Plan and Playbooks…

  And USE THEM during the exercise.
- Train like you fight! Communicate and act as if you were in a real incident.

SUMMARY - BENEFITS

The benefits of performing regular Tabletop Exercises:

- ❑ Validates plans & playbooks – pressure-tests documented procedures against realistic scenarios and reveals gaps before a real crisis.

- ❑ Enhances security culture – turns "security is everyone's job" from slogan into practiced muscle memory.

- ❑ Consistent skill retention – frequent practice keeps procedures and contacts fresh in memory, reducing on-call "rust."

- ❑ Increases alignment between enterprise and site/field level personnel

- ❑ Validates/verifies assessment levelsBy increasing the relevance, risk and downtime are reduced

SCENARIO OVERVIEW

Today, we're running a tabletop exercise for Praxima Midstream Energy — a midstream oil & gas company actively working to align with the NIST Cybersecurity Framework v2.0. We're going to look at how their governance and incident response programs function under two different maturity levels.

In the first scenario, Praxima is early in their CSF adoption. They have policies starting to form, but gaps still exist in roles, approvals, and decision ownership. We'll see how basic governance and escalation processes hold up when stressed.

In the second scenario, Praxima has invested heavily — they have policies, roles, access controls, and regulatory processes fully implemented. But now we test how well those processes actually function under real-world friction — vendor conflicts, regulatory gray zones, media pressure, and internal disagreements.
Both exercises focus on decision-making, policy execution, and cross-functional coordination under pressure — mapping directly back to CSF v2.0 governance and response subcategories.

SCALING TTX ACROSS CSF v2.0 MATURITY LEVELS

Category	Low Compliance	High Compliance
Compliance Maturity	Emerging CSF v2.0 Adoption	CSF v2.0 Tier 3-4 Mature
Focus of the Exercise	Establish Roles, Assign Ownership	Validate Execution of Policies
Primary Challenge	Who Decides?	How Well are Processes Followed?
Key Observables	Role Confusion, Missing Policies	Process Drift, Policy Application Debate
Inject Themes	Policy Gaps, Access Requests, Ransomware, Regulatory Uncertainty	Policy Execution, Vendor Conflicts, Communications, Regulatory Coordination
Facilitator Focus	Who Owns Decisions? What Policies Apply? Who Escalates?	Is Process Followed? Are SOPs Applied? Is Messaging Aligned?

TTX BUILD PROCESS

1

Reference Maturity Assessment Scores

- Pull your latest CSF v2.0 maturity assessment.

2

Select Target Areas

- Pick 1-3 categories needing improvement or validation.

3

Map to CSF v2.0 Subcategories

- Identify specific CSF v2.0 subcategories to focus the scenario.

4

Translate to ThreatGEN Inputs

- Tell ThreatGEN your current vs target maturity levels and focus areas.

5

Request ThreatGEN to Build Injects Around these Focus Areas or Make Your Own

- Tied to governance, response, vendors, comms, or escalation.

6

Or create injects that stress decision-making, policy execution, escalation, vendor coordination, and communication friction.

7

Review and Fine Tune Inject List

- Customize injects to match your environment, roles, and timing.

LIVE DEMO - CLINT BODUNGEN

UTSI INTERNATIONAL

Q&A

If interested in receiving a copy of this presentation, email Shaun Six at scs@utsi.com