U.S. DEPARTMENT OF
ENERGY

FAIRCON Event Series

Maturing A Quantitative Risk Management Program in the Federal Government

Presentation and Discussion with Ignatius Liberto, Department of Energy

DOE OCIO ECRM Team

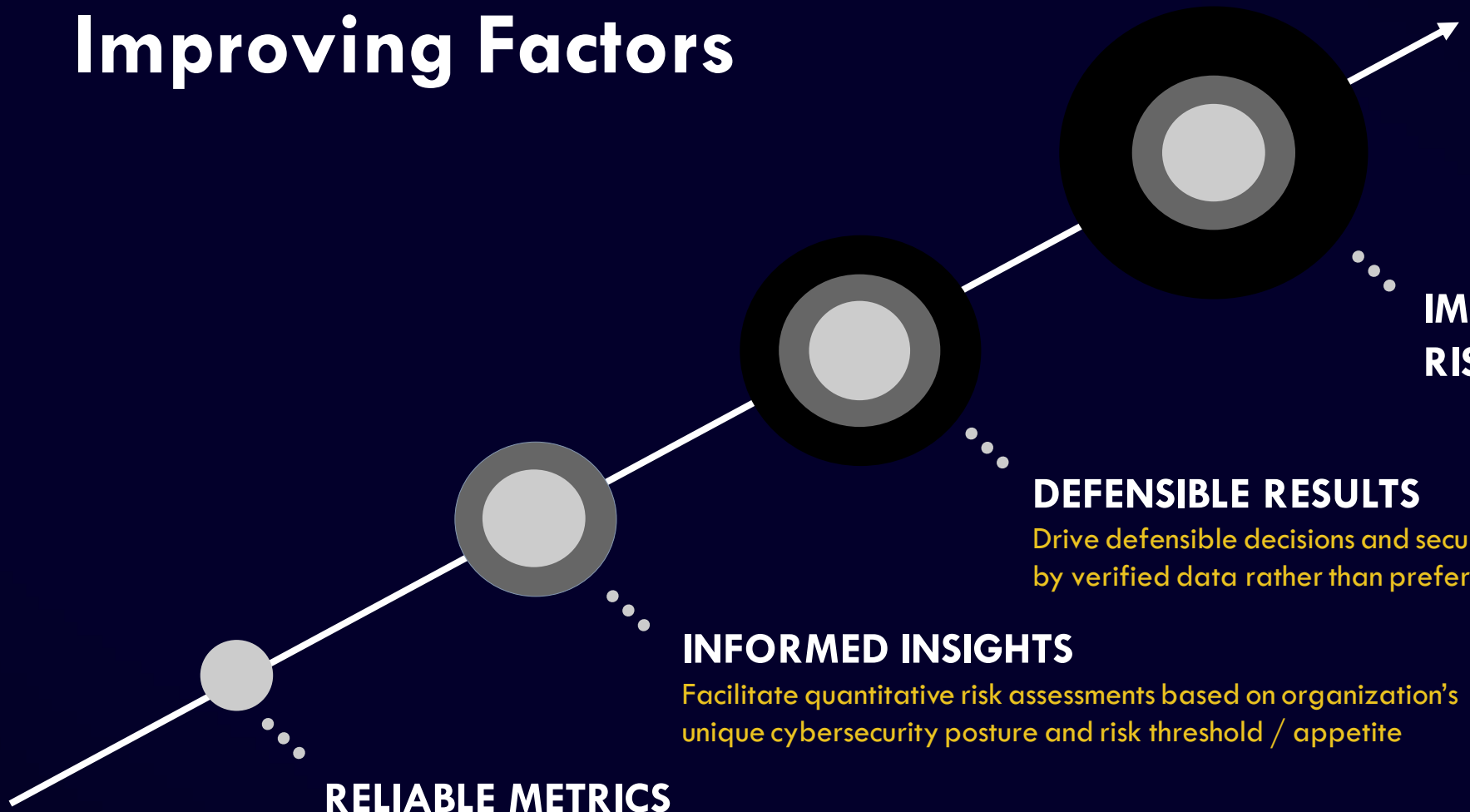
Ignatius Liberto
Director, IM-32
Department of Energy

Lili Cameron
Program Manager, IM-32
Department of Energy

Claudine Roxas
Strategy & Advisory Lead
Department of Energy

John Lamm
ECRM Team Lead
Department of Energy

Improving Factors



IMPROVED CYBERSECURITY RISK MANAGEMENT

DEFENSIBLE RESULTS

Drive defensible decisions and secure investment decisions driven by verified data rather than preferences or red herrings

INFORMED INSIGHTS

Facilitate quantitative risk assessments based on organization's unique cybersecurity posture and risk threshold / appetite

RELIABLE METRICS

Track measurable progress of risk mitigations and responses to minimize risk exposure and promote accountability

Keys to Maturing a Program

ANALYSIS COOPRATION
External assessments rely on participation and responsiveness of the stakeholder organizations

SCALABILITY AND ADOPTION
Translating analysis findings into applicable terms for your organization

TAILORING
Customizing FAIR language and training to the government space and missions; overcoming lack of industry standards

ADAPTABILITY
Customize industry best practices and methodologies to your organization's interests

Challenges: External Communication

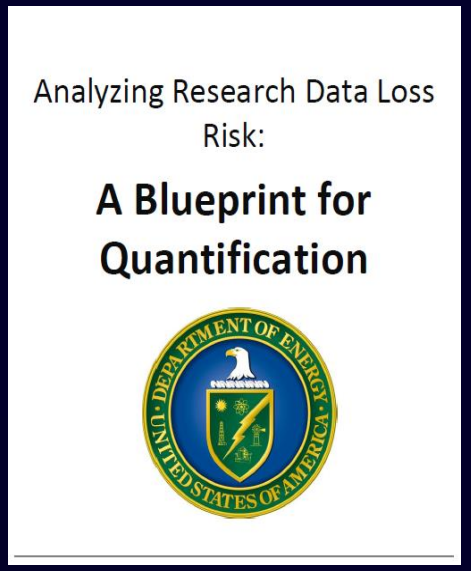
DATA GATHERTING
Getting cooperation and buy-in from subject matter experts and data owners

COMMUNICATING RESULTS
Translating analysis findings into applicable terms for your organization

RESOURCE MANAGEMENT
Clarifying expectations in resource-constrained environment with few dedicated risk analysts

External Communication Resources

Pitch risk management as an offering and fill in resource gaps by maximizing a team's efficiency with supportive materials and streamlined, replicable processes



Risk Assessment Blueprints
Provides sites and labs walkthroughs for scoping relevant topics as specified by DOE leadership

Program Placemat
Full overview of program goals, services, methodologies and objectives

Reporting Templates
To transform findings into recommendations, a visual breakdown of the analysis results is required

Challenges: Education

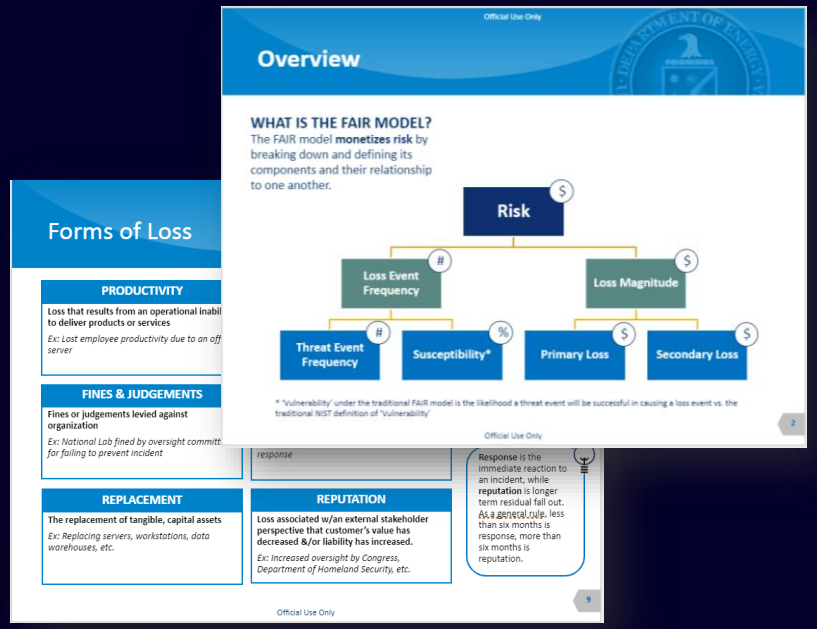
TIERED TRAINING
Targeting training to the right audiences

FEDERAL REQUIREMENTS/GUIDELINES
Incorporating quantitative risk management with Federal guidance

CALIBRATION TECHNIQUES
Teaching calibration in a way that is accessible and applicable

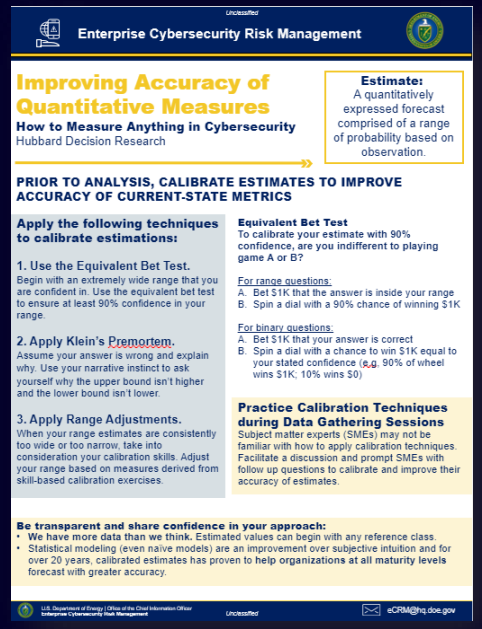
Education Resources

Recognize that risk management is not one-size-fits all for any organization or individual and offer customizable education



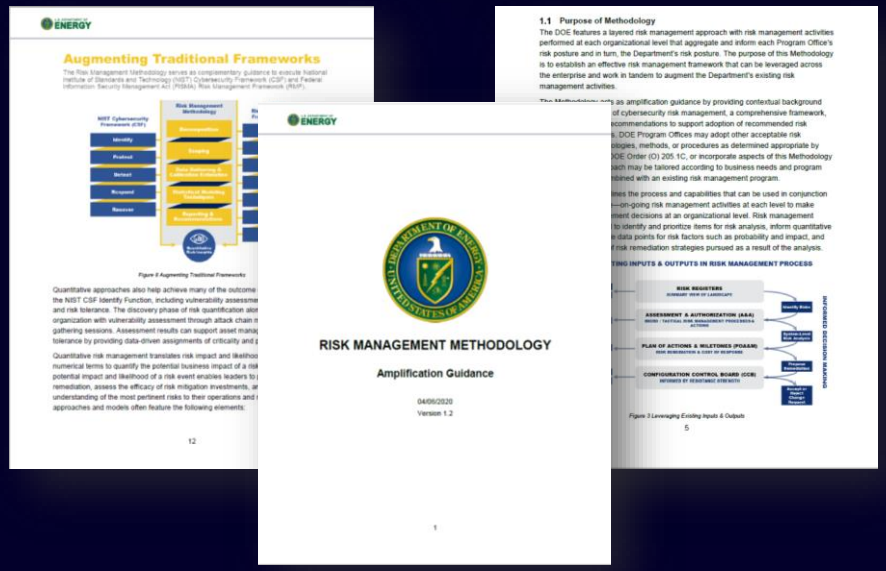
Introductory Deck

Introduction to FAIR and the foundations of quantitative risk management



Theme driven One Pagers

Overviews of best practices and techniques, such as calibration



Amplification Guidance

Risk management methodology and integration of relevant guidance and policies

Pragmatic Use Case

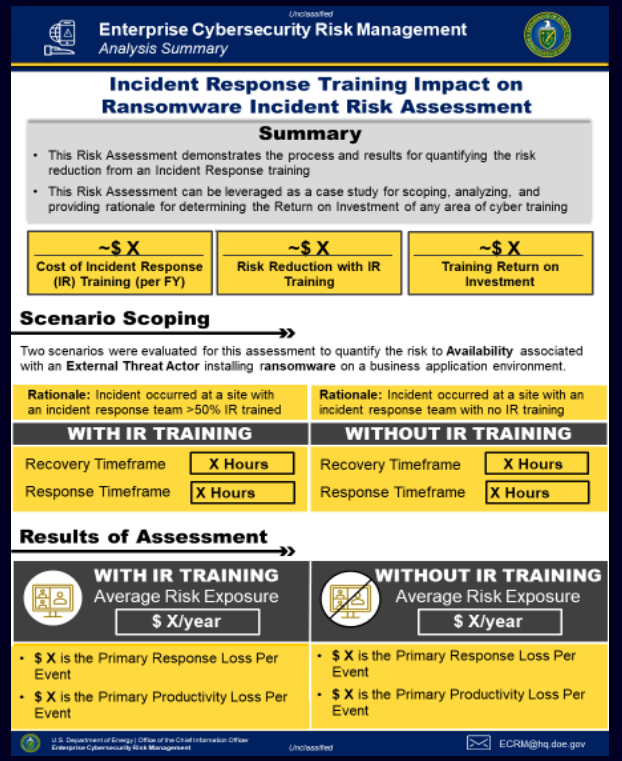
Assessment Summary

The ECRM team recommends continued investment in Incident Response Training, as even a modest predicted impact on the response time and recovery timeframe results in a significant ROI for training when experiencing a Ransomware incident for a GSS asset.

Justification of Decision

- Survey results from the Training and SOC SME interviews indicated at least a 15% improvement in response ability

- For the "With Incident Response Training" Scenario, it is assumed that the incident occurs at a laboratory with an incident response team with greater than 50% of members having attended the Incident Response Training
-
- This improvement is reinforced by the participant surveys. 100% of DOE survey participants who completed the Incident Coordination Training responded positively to the survey questions.



Key Takeaways

USE CASES

Let your tactical success drive your program.

Don't get hung up on an enterprise-wide silver bullet strategy. Find tactical applications for the work and employ quantitative risk management for specific use cases to meet demands of your stakeholders.

TEMPLATES

Build a library of tailorable templates to help lighten the load for your resources.

Use these templates to guide analyses and streamline reporting and training.

EXECUTIVE MESSAGING

Develop talking points and field-tested / effective language that can be tailored for different types of leadership.

Customize based on the priorities of the organization and include tactical success stories.

For additional information:
Email the DOE ECRM Team (ecrm@hq.doe.gov)