MODERN TECHNOLOGY SOLUTIONS, INC.®

# Using Probabilistic Mission Risk Analysis (PMRA) to Present Testing Data

"All models are wrong, but some are useful"
—George Box

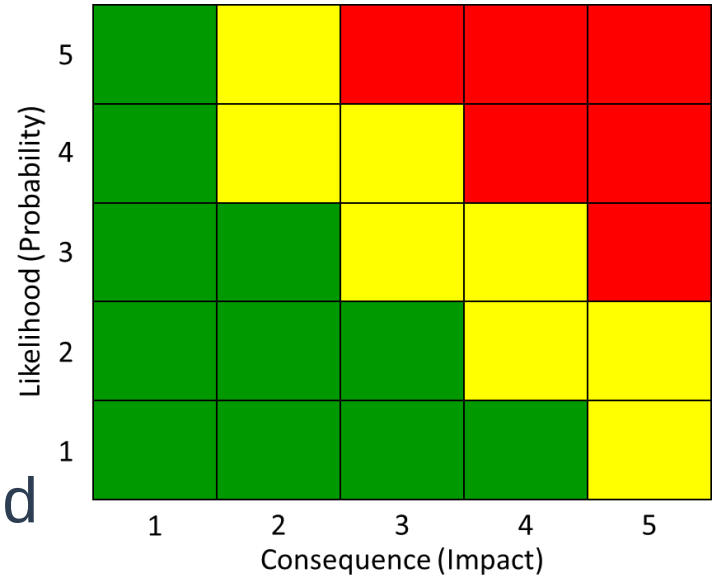
Dr. Bill "Data" Bryant
bill.bryant@mtsi-va.com

# What's the Problem?

- Weapon systems and platforms are vulnerable to cyber attack
  - ICS/SCADA attacks—STUXNET, Black Energy, etc.
  - Car and aircraft hacking demonstrations
- No widely accepted way to present test data
  - Different organizations are using very different methodologies
  - Makes comparison across systems very difficult
  - Quantitative vs. qualitative debate rages on
- Often unclear to stakeholders what the cyber test results mean for the mission
- There is typically no uncertainty or confidence interval associated with cyber testing

# Current Approach Issues

- Most common approaches used today to measure risk to weapon systems involve ranking likelihood and consequence 1-5 and plotting on “Risk Cubes”
- Numerous issues with this approach
  - Ordinal vs. ratio scale makes arithmetic combining invalid
  - No research evidence showing this approach is effective
  - What research does show
    - Cognitive bias issues and overconfidence
    - Inconsistency in scoring even using strict categorization
    - Range compression
    - Multiple areas on risk cubes where they cannot unambiguously score randomly selected pairs of hazards
    - Users feel better about risk, even if they don’t understand it better



# LENSES ON RISK

- The Institute for Defense Analysis (IDA) did a study to compare various mission based cyber risk methodologies
  - Found more than 20 unique methodologies in use
  - Most of the models included the same three elements combined in different ways to get to a two-dimensional risk cube
- The three common elements are
  - Criticality
  - Threat
  - Vulnerability
- The first step of PMRA is to analyze the risk to the system and mission using all three lenses

# CRITICALITY

- Most often, programs today analyze their architecture to try to identify what components are “critical”
  - For weapon systems with significant size weight and power constraints, if it wasn’t mission critical, it was never in the design
  - When everything is critical, then nothing is critical
- Some systems have a natural hierarchy of criticality, losing mission capability is most often less critical than losing the system permanently with potential loss of life
- One possible scoring method is

| | |
|---|---|
| Tier 1 | Loss of component/function would likely result in the death of friendly or neutral personnel |
| Tier 2 | Loss of component/function would likely result in the permanent destruction of the weapons system |
| Tier 3 | Loss of the component/function would likely result in complete loss of the mission capability (no-potential work-arounds) |
| Tier 4 | Loss of the component/function would likely result in a partial loss of the mission capability |
| Tier 5 | Loss of the component/function would not change expected mission effectiveness |

- Do an engineering analysis and determine what sub-systems and components are most critical

MODERN TECHNOLOGY SOLUTIONS, INC.®

# THREAT

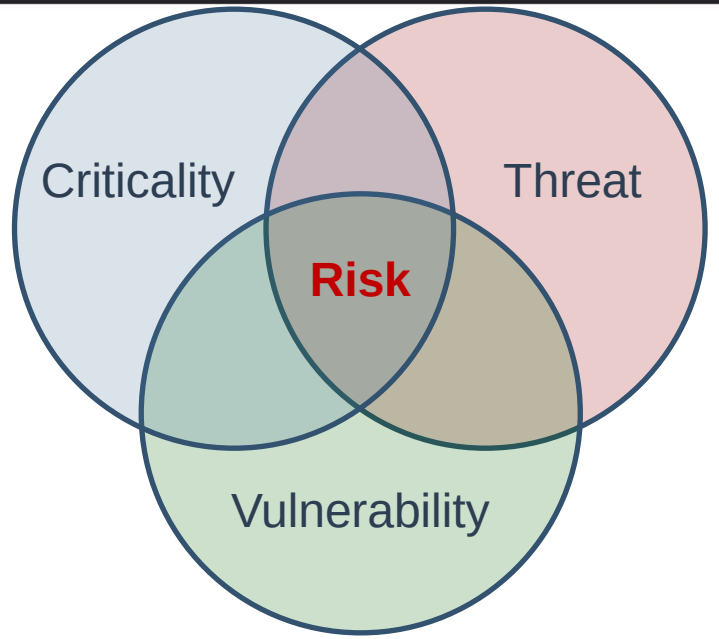
- Two major components to threat
  - Capability
  - Intent
- Both are specific to a particular scenario and threat actor
- Finding enemy battleships is relatively easy
  - Enormous physical “thing” with thousands of people working on it requiring thousands of tons of steel, etc.
- Finding enemy cyber weapons is not
  - Small group of people in an isolated network physically located in any non-descript office building can develop a cyber weapon
- As a result, while threat intelligence is tremendously important, never assume you know very much about adversary cyber weapons
- May have to rely on plausibility versus specific intent

# VULNERABILITY

- "Vulnerability" has many different definitions
  - CNSSI 4009: "Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source."
  - Does not have to be technical
- Many different types of vulnerabilities including supply chain, development, software, hardware, etc.
- Many different tools are available to help find vulnerabilities
  - Architectural analysis
  - Static and dynamic code analysis
  - Fuzzing
  - Red teams
- Product of analysis should be a list of known or potential vulnerabilities with some ranking of severity

# Developing Risk Scenarios

- A risk only occurs at the intersection of criticality, threat and vulnerability
- When developing risk scenarios it is normally helpful to spend some time developing scenarios starting with each of the three lenses




- Risk scenario = story of a potential ***threat*** exploiting a ***vulnerability*** to impact a ***critical*** sub-system or component
- Tools exist that can help
  - Systems-Theoretic Process Analysis for Security (STPA-Sec)
  - Cyber Table Top (CTT)
  - Red team reports and known historical attacks

# Scoring Risk Scenarios

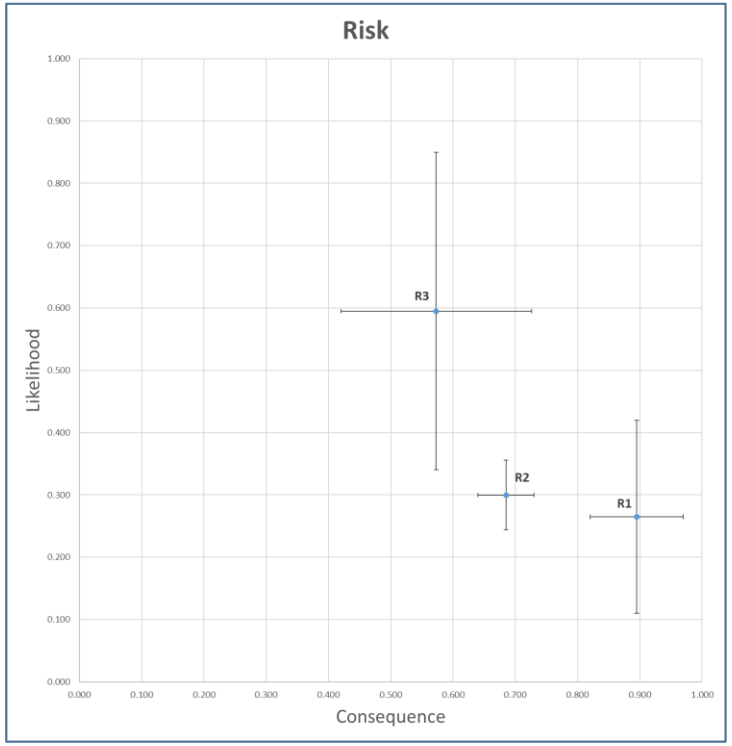
- Qualitative vs. Quantitative
  - We want to be as quantitative as possible, but no more
  - Balance will often change throughout lifecycle
- To be able to combine scores arithmetically we need to use a ratio instead of an ordinal scale
  - Differences between values on the scale are meaningful
  - True zero
- Need to combine likelihood (how likely a particular scenario is to occur) with consequence (how much mission is lost if a scenario does occur)
- Likelihood is measured as a probability (0 - 100%)
- Mission loss is measured as a percentage (0 - 100%)

# LIKELIHOOD

- Cyber attack risk scenarios have a high level of uncertainty and limited data sets
- Fortunately, Applied Information Economics (AIE) was developed to measure probabilities in environments with high uncertainty and includes several key components
  - Probability distributions: Instead of assigning point probabilities, AIE uses 90% probability distributions as inputs
    - Can be based on a large number of different distributions—normal may not be the right answer depending on the underlying data
  - Expert calibration: Proven process to teach subject matter experts to more correctly assess their own accuracy
  - Monte Carlo simulations: Developed during the Manhattan project to combine probabilities—easily accomplished in Excel
- Each risk scenario likelihood is given a 90% Probability Distribution (PD) based on a selected distribution

# CONSEQUENCE

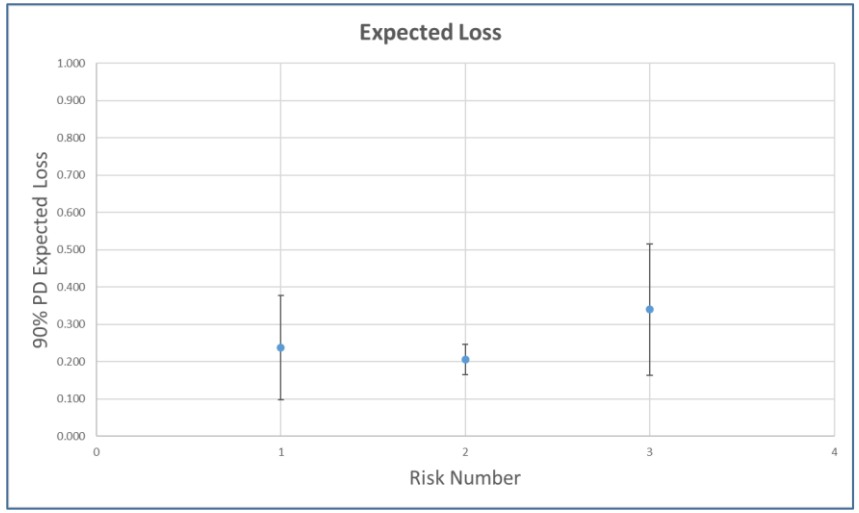
- If the risk scenario occurs how much mission is lost?
  - Sometimes is much simpler than more generic impact measurements—if all of the flight controls on an aircraft are lost then the mission loss = 100%
  - May need to average across multiple mission types depending on the design requirements
- Likelihood and consequence charted on a 2-D graph
- Differences from Risk Cube:
  - Scores on axes are continuous
  - Results include 90% PD error bars that explicitly show the level of confidence in the score
  - Risk scores can be meaningfully compared



# Expected Loss

- Expected loss is the sum of all the values of all possible losses, with each multiplied by the probability of that loss occurring
  - In the finance world, this is often used in lending
- We now have all the data needed to calculate expected loss for each scenario as well as overall
  - If point values are desired, simple multiplication will suffice, otherwise another Monte Carlo simulation will give a probability distribution

| | | Mean EL | 90% PD EL Lower | 90% PD EL Upper |
|---|---|---|---|---|
| **R3** | Steal Mission Data | 34.1% | 16.8% | 51.4% |
| **R1** | Capture Air Vehicle | 23.6% | 9.7% | 37.5% |
| **R2** | Malicious Parachute Deploy | 20.6% | 16.5% | 24.7% |

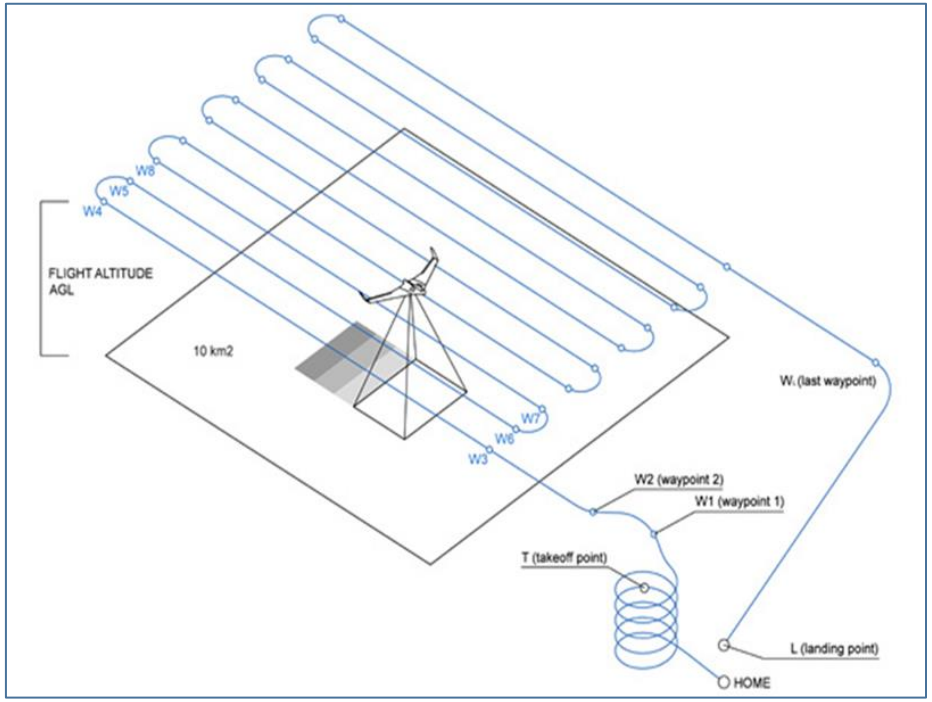


# PMRA and Testing

- While PMRA utilizes SME assessment to develop the probabilities for likelihood and consequence, include test data whenever possible
- Testing can help identify new risk scenarios
- Testing can help improve scoring
  - Normal nation state attackers will have far greater resources and time than testers so if testers get in via a route considered to have a low probability, the probability is likely optimistic
  - Testing can also illustrate unexpected system connections and behavior that can raise or lower expected consequence
- If risk scenarios have an unacceptably high level of uncertainty, testing can reduce that uncertainty
  - Should be a feedback loop between risk management, design efforts, & testing

# UAS EXAMPLE

- UAS system under consideration is a blended wing body Air Vehicle (AV), ground station, and launching catapult
- Intended for precision air surveying missions

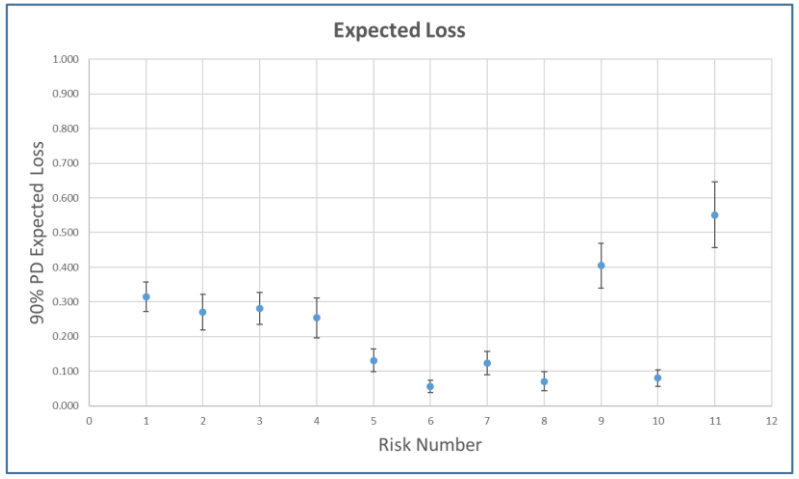


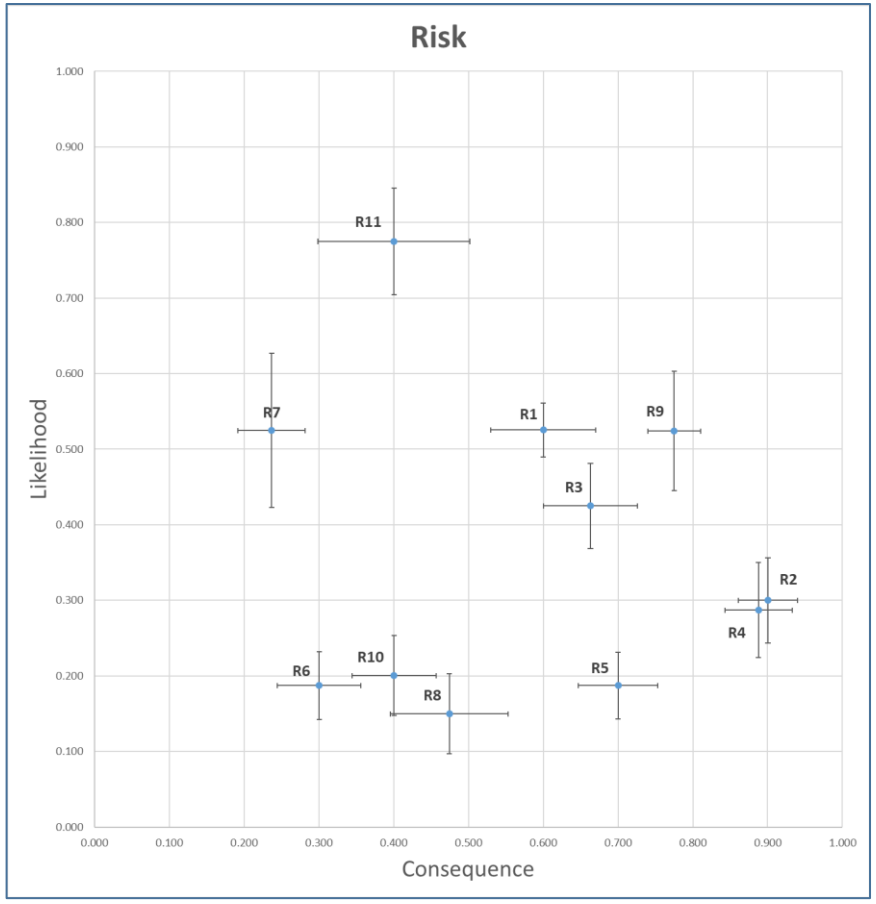

- Typical mission profile includes
  - Catapult launch
  - Autonomous flight operations to perform survey work under direct observation by the pilot
  - Recovery via parachute descent
- Pilot can assume control at any time by providing mission updates or simple commands

# UAS EXAMPLE

- This study included both cyber and EW risks
- High uncertainty may point to areas where testing would be valuable

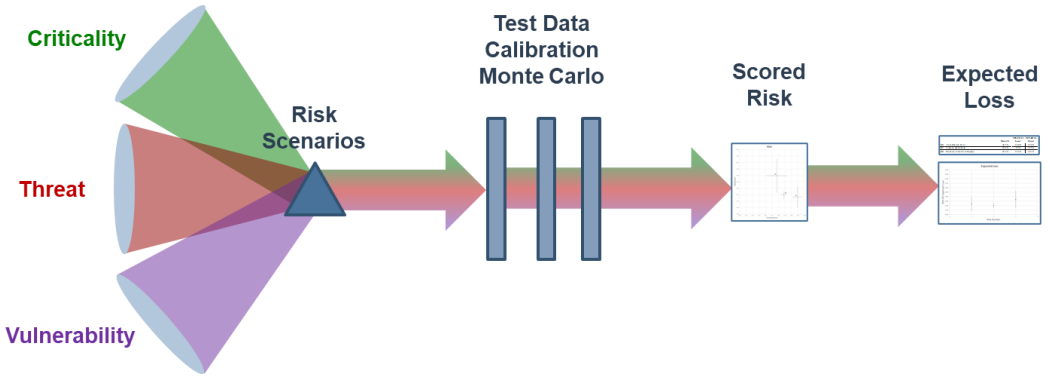
| | | Mean EL | 90% PD EL Lower | 90% PD EL Upper |
|---|---|---|---|---|
| **R11** | GPS Jamming | 55.2% | 45.9% | 64.5% |
| **R9** | Malicious Parachute Deploy | 40.6% | 34.2% | 46.9% |
| **R1** | Communication Jamming | 31.5% | 27.2% | 35.7% |
| **R3** | Competing Ground Station Crash | 28.2% | 23.6% | 32.8% |
| **R2** | Capture Air Vehicle | 27.0% | 21.9% | 32.2% |
| **R4** | Competing Ground Station Targeted Crash | 25.4% | 19.7% | 31.2% |
| **R5** | Manipulate Commands on Ground Station | 13.1% | 9.8% | 16.4% |
| **R7** | Command Replay to Air Vehicle | 12.4% | 9.0% | 15.8% |
| **R10** | Malicious Camera Commands | 8.0% | 5.6% | 10.4% |
| **R8** | Manipulate Air Vehicle Status on Ground Station | 7.1% | 4.3% | 9.9% |
| **R6** | Steal Data from Ground Station | 5.6% | 3.9% | 7.3% |



# CONCLUSIONS

- PMRA avoids many of the pitfalls in risk cubes without requiring more resources
  - Scoring still done by SMEs
  - SMEs are trained to reduce bias and errors
- PMRA ensures scenarios represent real risk with threat, vulnerability, & criticality




- PMRA is displayed in a format easily understandable by senior leaders used to looking at risk cubes
- PMRA overtly shows how much uncertainty there is in a risk measurement instead of hiding it behind a point value
- PMRA enables better communication of the risk associated with a system based on cyber testing results and how it impacts the mission

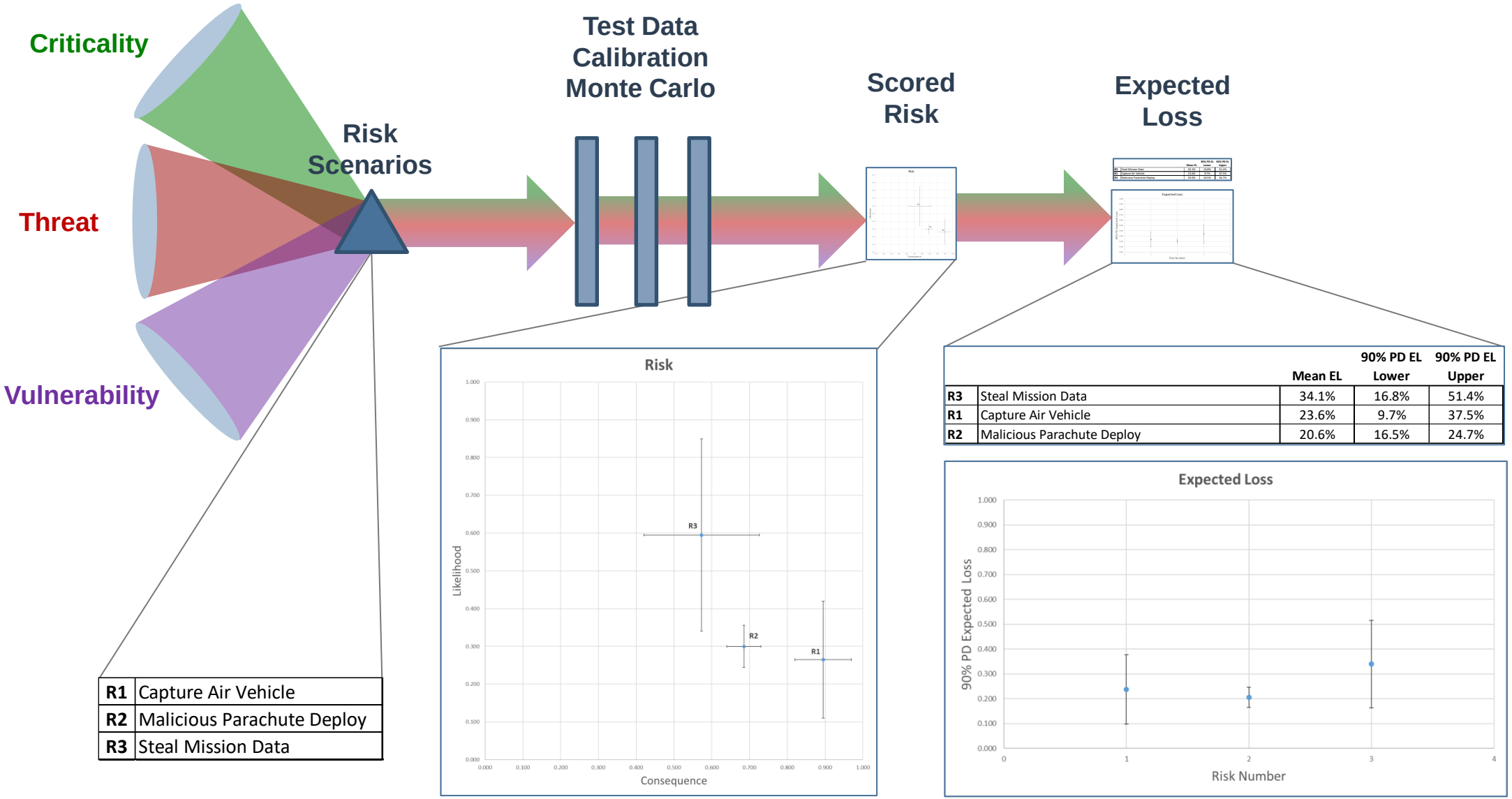
MODERN TECHNOLOGY SOLUTIONS, INC. ®

# Thank you for your time

## Please reach out with any questions

**Dr. Bill “Data” Bryant**
bill.bryant@mtsi-va.com

# PROBABILISTIC MISSION RISK ANALYSIS (PMRA)




| | | Mean EL | 90% PD EL Lower | 90% PD EL Upper |
|---|---|---|---|---|
| **R3** | Steal Mission Data | 34.1% | 16.8% | 51.4% |
| **R1** | Capture Air Vehicle | 23.6% | 9.7% | 37.5% |
| **R2** | Malicious Parachute Deploy | 20.6% | 16.5% | 24.7% |

| | |
|---|---|
| **R1** | Capture Air Vehicle |
| **R2** | Malicious Parachute Deploy |
| **R3** | Steal Mission Data |