WELCOME! MEASUREMENT PLANNING FOR FAIR

TODAY'S GOAL: Enhanced understanding of scenario-construction, structuring, and planning related barriers to successful decision support, techniques for overcoming those barriers, and a conceptual framework for operationalizing those techniques.

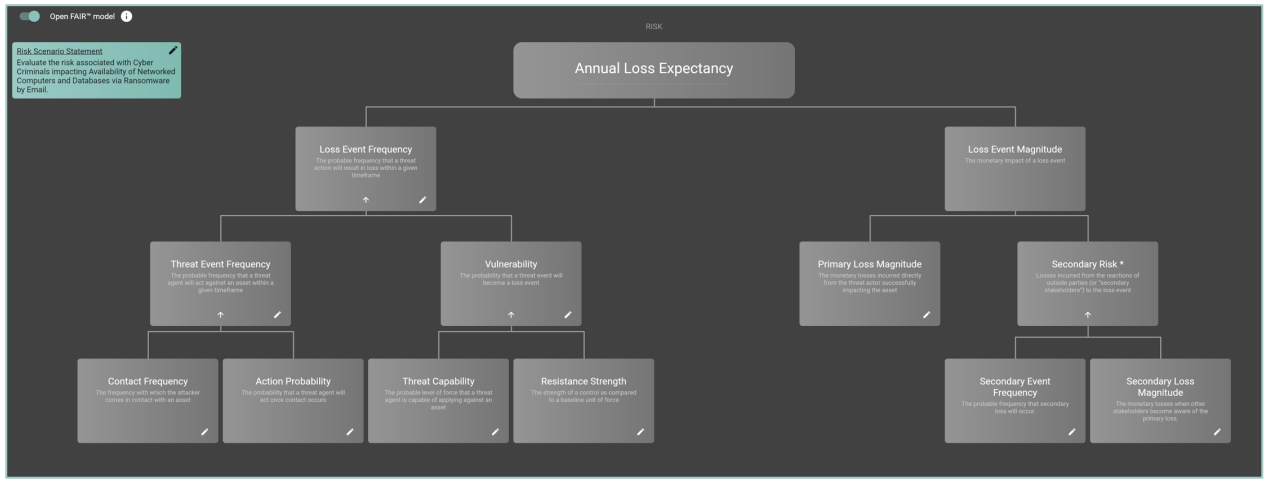
WHY? Quantifying one scenario once is relatively easy. Providing useable decision support with CRQ over time and scale becomes increasingly complex and needs to be planned with intent.

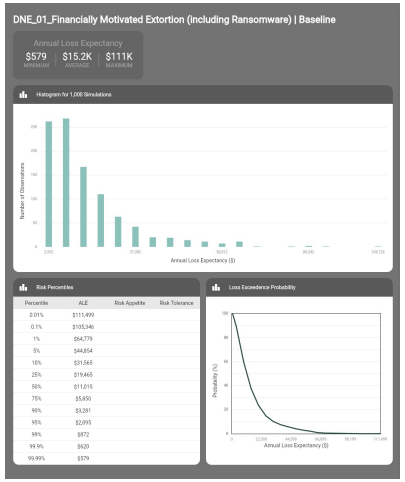
Jack Whitsitt | Director of CRQ at Ostrich Cyber-Risk | jack.Whitsitt@ostrichcyber-risk.com

SCOPING AND QUANTIFYING *A* SCENARIO

FAIR SCENARIO

- Threat Community
- Threat Event
- Asset
- Loss Event





HAVE YOU CONSIDERED YOUR CONSTRAINTS?

IMPOSED REQUIREMENTS

- Environmental/Org Specifics
- Decision Support Criteria
- “Reporting Formats”
- Operating Business Constraints

IMPLICIT REQUIREMENTS

- Measurement Integrity
- Domain Model Accuracy (Infosec / Business)

ANALYTIC REQUIREMENTS

- Process & Resource Constraints
- Scope to Scenario to Factor to Indicator Model
- Estimation Model Choices

HAVE YOU CONSIDERED ALL OF YOUR CONSTRAINTS?

Decision Support Criteria Set 1
Decision Support Criteria Set 2
Decision Support Criteria Set 15

Environmental Specifics Last Year
Environmental Specifics Today
Environmental Specifics Next Week

"Reporting Formats" For Stakeholder Set 9
"Reporting Formats" For Stakeholder Set 1
"Reporting Formats" For Stakeholder Set 2

Business Constraints Today
Business Constraints Next Quarter
Business Constraints Yesterday

IMPLICIT REQUIREMENTS

- Measurement Integrity
- Domain Model Accuracy (Infosec / Business)

ANALYTIC REQUIREMENTS

- Process & Resource Constraints
- Estimation Model Choices

WE ALSO HAVE STRUCTURAL CO-DEPENDENCIES

- Individual Scenarios
- Scenario Sets (Must Work Jointly)
- Estimation Model Choices
- Data Source & Applicability Choices
- Reporting Choices

FEATURES (NOT BUGS) OF FAIR THAT MAKE THIS HARD

1. FAIR IS LOSSY: World->Scenario->Factors->ALE but not reverse
2. FAIR IS FLEXIBLE: But approaches end up bespoke
3. FAIR IS ONTOLOGICALLY SOUND: Human thinking is not
4. FAIR MEASURES ACTUALS: And that's not always what's available

SO WHAT DO WE DO?

Proper Measurement Planning can combine and simplify requirements where possible to maximize the degree to which CRQ requirements can be met by a given set of resources with a single approach and a common set of scenarios.

We can reduce the impact of constraint variance over time, improve quality and efficiency, and improve ability to estimate and describe resource requirements.

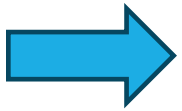
WHAT GOES INTO A MEASUREMENT PLAN?

Remember these?

IMPOSED REQUIREMENTS
- Environmental/Org Specifics
- Decision Support Criteria
- "Reporting Formats"
- Operating Business Constraints

IMPLICIT REQUIREMENTS
- Measurement Integrity
- Domain Model Accuracy (Infosec / Business)

ANALYTIC REQUIREMENTS
- Process & Resource Constraints
- Scope to Scenario to Factor to Indicator Model
- Estimation Model Choices



Plan Manages Constraint Coordination

(Example) MEASUREMENT PLAN STEPS

1. Document & Maintain Environmental/Org Specifics | *Routine*
2. Create/Execute Decision Support Criteria Management Cycle | *Annual*
3. Manage & Maintain CRQ Output Reporting Templates vs Others | *Routine*
4. Identify, Document, Communicate Business Constraints | *Annual?*
5. Manage "Scenario Set Design" lifecycle (Implicit/Analytic) | *Annual*
6. Manage "Theory of Risk Design" lifecycle (Implicit/Analytic) | *Annual*
7. Derive Standing "Data Requirements" to be fulfilled at cadence | *Annual*
8. Document gaps -> Start new plan if needed | *at Ops Cadence*

1. "Ops": Data Gathering / Quant / Analyze / Report / Support | Quarterly?
2. Intermittent Updates: Use Existing to Provide Ad-Hoc Support

IMPOSED REQUIREMENTS: Environmental/Org Specifics

"ABOUT US"

	Current Information	Refresh Process	POCs
People, Process, Technology, Data			
Security Equities & Stakeholders			
Enterprise Risk & BIA Scenarios			
Strategic Threat Landscape			
TTP & Surface Sets			
Control Framework			
Data Sources			

"REFERENCE CLASS LEXICON"

LOSS MAGNITUDE SCOPE

Stakeholders	Business Outcomes	Stakeholder Expectations	Loss Scenarios	Cost Drivers
_Any	_Any	_Any	_Any	_Any
_All	_All	_All	_All	_All
Community	AVAILABILITY: _ANY	Accurate and secure financial information	_NONE ***	Capital Expense Increase

SUSCEPTIBILITY SCOPE

Initial Access VECTORS	Assets	Threat Events / Actions on Objectives	Surface Areas	Control Domains (Whatever the NISTCSF Term Is)
_All	_All	_All	ASDESIGNED: _Any	Analysis (RS.AN)
_Any	_Any			
_Other	_Other			
Phishing: Bespoke	TECHNIC			
Phishing: Focused	TECHNIC			
Phishing: General	TECHNIC			
Public Facing Services	TECHNIC			
Supply Chain Insertion	TECHNIC			
Third Party Credential Compromise	TECHNIC			
Verbal Social Engineering	TECHNIC			
Insider Collaboration	CONTENT			
	CONTENT			
	CONTENT			
	CONTENT			
	CONTENT			
	CONTENT			
	PROCESS			
	PROCESS			
	PROCESS			
	PROCESS			
	PROCESS			
	HUMAN:			
	HUMAN:			
	HUMAN:			
	HUMAN:			
	HUMAN:			
	HUMAN:			
	HUMAN:			

THREAT EVENT FREQUENCY SCOPE

Threat Motivations	Threat Communities	Target Criteria	Initial Access LEVELS
_All	_All	_All	_All
_Any	_Any	_Any	_Any
_Other	_Other	_Other	_None
Coincidental: _All	Hacktivists: _All	Data: _All	_Other
Coincidental: _Any	Hacktivists: _Any	Data: _Any	Contact: Routable
Coincidental: _Other	Hacktivists: _Other	Data: _Other	Full: Supply Chain Trust
Espionage (Non-Conflict): _All	Hacktivists: Coordinated Unaffiliated Groups	Data: Marketable (any type)	Full: System Root/Admin
Espionage (Non-Conflict): _Any	Hacktivists: Lone Wolf	Data: Opportunistic	Full: User Credentialed
Espionage (Non-Conflict): _Other	Hacktivists: Sponsored	Data: Owner Ops-Critical	Some: Credentialed
Espionage (Non-Conflict): Corporate/Private	Legitimate Access Actors: _All	Data: Owner-Sensitive	Some: Supply Chain Trust
Espionage (Non-Conflict): Geopolitical	Legitimate Access Actors: _Any	Data: Threat-Useful	Some: System User
Financial: _All	Legitimate Access Actors: _Other	Data: Volume	
Financial: _Any	Legitimate Access Actors: Contractors	Human: _All	
Financial: _Other	Legitimate Access Actors: Employees	Human: _Any	
Financial: Data Sale	Legitimate Access Actors: Supply Chain	Human: _Other	
Financial: Extortion: _All	Legitimate Access Actors: Vendors	Limited Resources: _All	
Financial: Extortion: Availability	Nation States: _All	Limited Resources: _Any	
Financial: Extortion: Confidentiality	Nation States: _Any	Limited Resources: _Other	
Financial: Extortion: Integrity	Nation States: _Other	Process: _All	
Financial: Fraud: Business Function/Process	Nation States: China	Process: _Any	
Financial: Fraud: Technical Function/Process	Nation States: Iran	Process: _Other	
Geopolitical Conflict: _All	Nation States: North Korea	Process: Business Function	
Geopolitical Conflict: _Any	Nation States: Other	Process: Technical Function	
Geopolitical Conflict: _Other	Nation States: Russia	Process: Vulnerable Surface	
Geopolitical Conflict: Damage	Nation States: Ukraine	Technology: _All	
Geopolitical Conflict: Demonstration/Threat	Nation States: United States	Technology: _Any	
Geopolitical Conflict: Future Positioning	Organized Criminals: _All	Technology: _Other	
Red Herring	Organized Criminals: _Any	Technology: Architecture: Public Facing	
Red Herring: _All	Organized Criminals: _Other	Technology: Business Function	
Red Herring: _Any	Organized Criminals: Access Resellers	Technology: Business Function: Customer Critic	
Red Herring: _Other	Organized Criminals: Informstion Resellers	Technology: Opportunistic	
Technical Resource Theft: _All	Organized Criminals: Ransomware Gangs	Technology: Stack	
Technical Resource Theft: _Any	Organized Criminals: Thieves	Technology: Technical Function	
Technical Resource Theft: _Other	Unaffiliated Malicious: _All	Technology: Vulnerable Surface	
Technical Resource Theft: Bandwidth	Unaffiliated Malicious: _Any		
Technical Resource Theft: Processing	Unaffiliated Malicious: _Other		
Technical Resource Theft: Storage			
Thematic: _All			
Thematic: _Any			
Thematic: _Other			
Thematic: ESG/Political			
Thematic: Nationalist			
Thematic: Personal			

IMPOSED REQUIREMENTS: Decision Support Criteria

		Depth / Precision
Breadth	Threat Commmunities	
	Motives	
	Target Criteria	
	Initial Access Vectors	
	Key Assets	
	Key TTPs	
	Key Surfaces	
	Key Controls	
	Key Business Events	
	Key Security Equities	
	Key Stakeholder Reactions	
	And So On	

	Group By Theme	Depth/Precision
Aggregate		
Time Trend		

	Fixed/Assumed	Variable
Residual		
A/B		

	Group By	Loss Counting Scope	Threshold
Tail Impact (STORM)			
Smoothed Impact (ALE)			

DECISION CONTENT:

- What needs to be in the scenario(s)?
- Where can we *stop* with precision and detail?

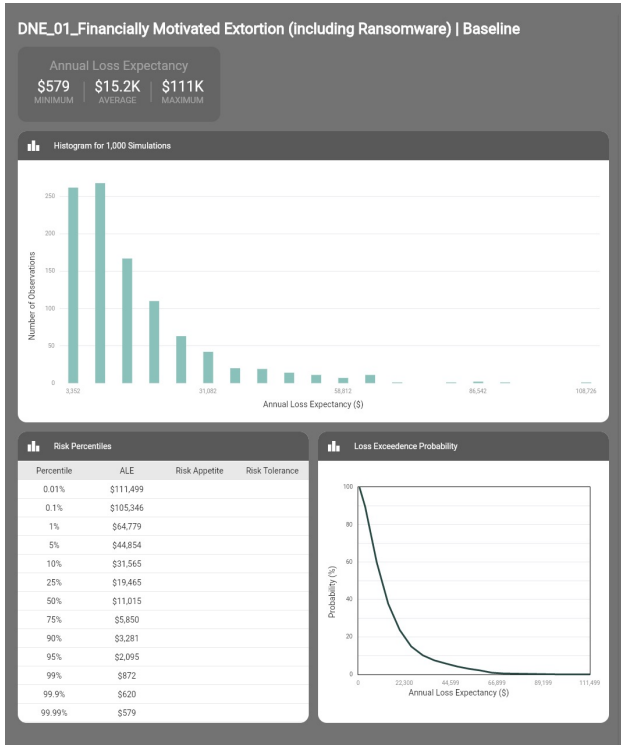
REPORTING APPROACH:

- What needs to be compared?
- What needs to be combined?

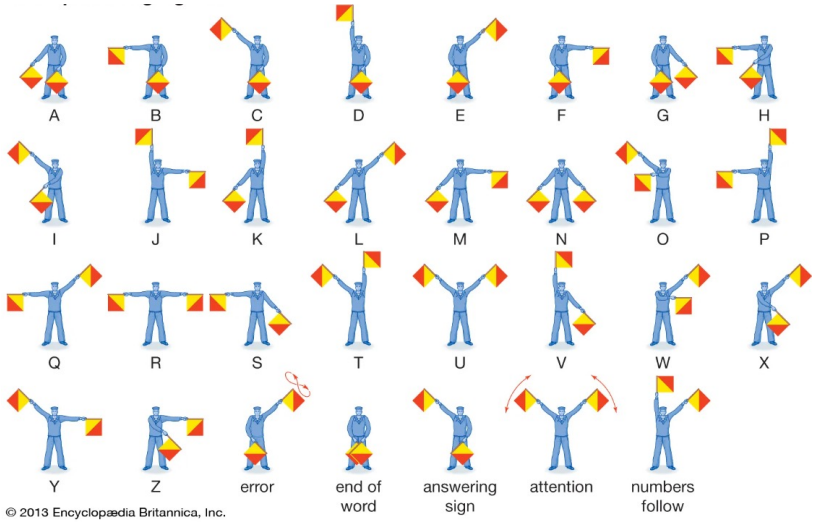
DECISION BASIS:

- Decision Indicators?
- Decision Metrics?

IMPOSED REQUIREMENTS: “Reporting Formats”



	Insignificant 1	Minor 2	Significant 3	Major 4	Severe 5
5 Almost Certain	Medium 5	High 10	Very high 15	Extreme 20	Extreme 25
4 Likely	Medium 4	Medium 8	High 12	Very high 16	Extreme 20
3 Moderate	Low 3	Medium 6	Medium 9	High 12	Very high 15
2 Unlikely	Very low 2	Low 4	Medium 6	Medium 8	High 10
1 Rare	Very low 1	Very low 2	Low 3	Medium 4	Medium 5



Wok wok wok wok….In this scenario, the same cybercriminal group as in the previous scenarios targets an organization, but with a different approach. They gain initial access to the network through a supply chain attack, compromising a third-party vendor's systems. The attackers then leverage this access to infiltrate the targeted organization's network. Once inside, they deploy ransomware, but instead of encrypting the data, they steal sensitive information and threaten to release it publicly unless a ransom is paid. The organization faces potential reputational damage, financial loss, and legal consequences….wok wok wok wok

IMPOSED REQUIREMENTS: Business Constraints

Compliance	
Culture Alignment	
Assumption Consensus	
Process Integration	
Consumers & Purposes	
Production Cadence	
Transparency	
Efficiency	
Version Control	
Communication Channels	
Business Lifecycle	

IMPLICIT & ANALYTIC REQUIREMENTS:

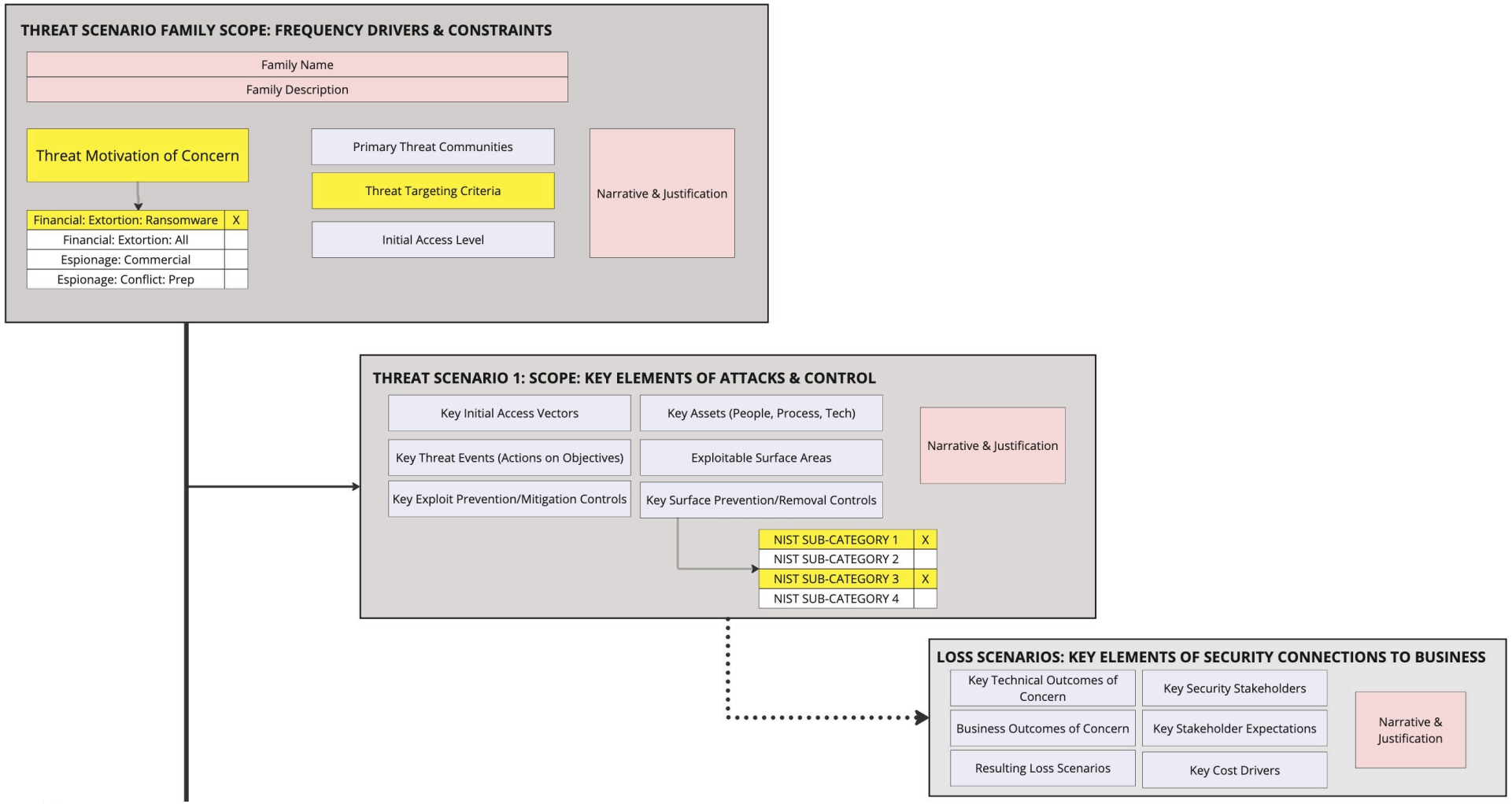
Scenario Set Design: Process, Resource, Measurement Constraints

- **Systems Modeling:**
  - Scenarios describe a situation (Dimensions and Units)
  - Stocks/Flows describe how it may vary and impact FREQ/MAG
  - Stressors/Inputs describe why and when FREQ/MAG may vary
  - Metrics/Measures describe by how much

System Description
Stock/Flow Variables
Stressors
Causative Drivers (Indicators)
Indicator Sources of Record
Measures & metrics

- **Modularity (LEGOS):** Sticky Data, Recombination, Aggregation, etc
- **Sample Sets for Ranges:** Representative down to decision precision (DJI)
- **Reference Classes:** I know something about sub-classes, super-classes, peer classes
- **Scenario Families:** Assure common purpose but along measurement rigor lines (oversampling protection)
- **Scenario Sets:** represent the widest ranges for factors needed for the broadest decision and reporting criteria that need to be combined

IMPLICIT & ANALYTIC REQUIREMENTS:
Requirements Scenario Example

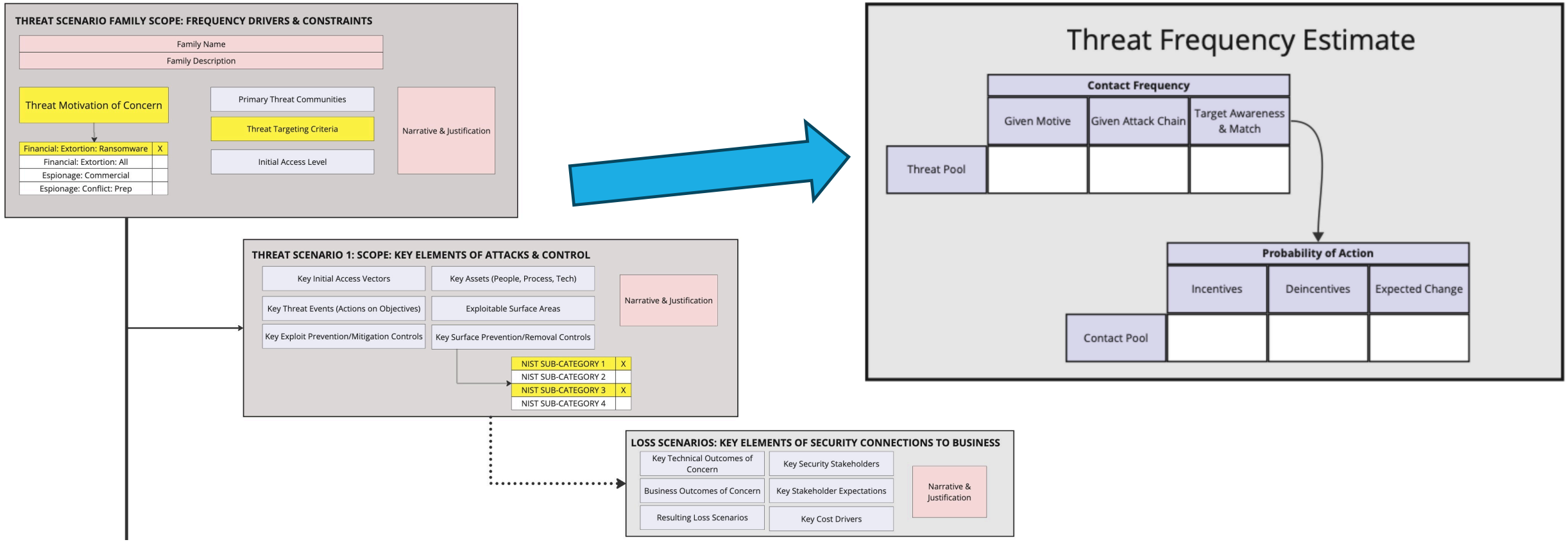


IMPLICIT & ANALYTIC REQUIREMENTS:

Stack requirements into common ranges where constraints allow.
Create additional scenarios only when needed.

IMPLICIT & ANALYTIC REQUIREMENTS

Theory of Risk Design: Model Accuracy, Estimation Models, Data Sources



- Estimation Models Need to be documented and re-used
- **Estimation Models affect how scenarios are built, what data is required, and vice versa -> Back-test!!**
- Modularity and Coherent Structure over time allows for standing “Data Sources of Record” vs “Go find data where you can”

PLAN MODEL: PLEASE DON'T DO ALL OF THIS! ☺

CRQ Measurement Planning

	Models	I/O	Metrics	Process	Stakeholders / RACI	Tools & Views	Maturity Plan
Environmental Specifics							
Decision Alignment							
Reporting Formats							
Business Constraints							
Scenario Set Design							
Theory of Risk Design							

Data Requirements

CRQ Operations

THANK YOU! QUESTIONS?

Jack Whitsitt
Director of CRQ at Ostrich Cyber-Risk
jack.Whitsitt@ostrichcyber-risk.com

Ask me about additional upcoming webinars!

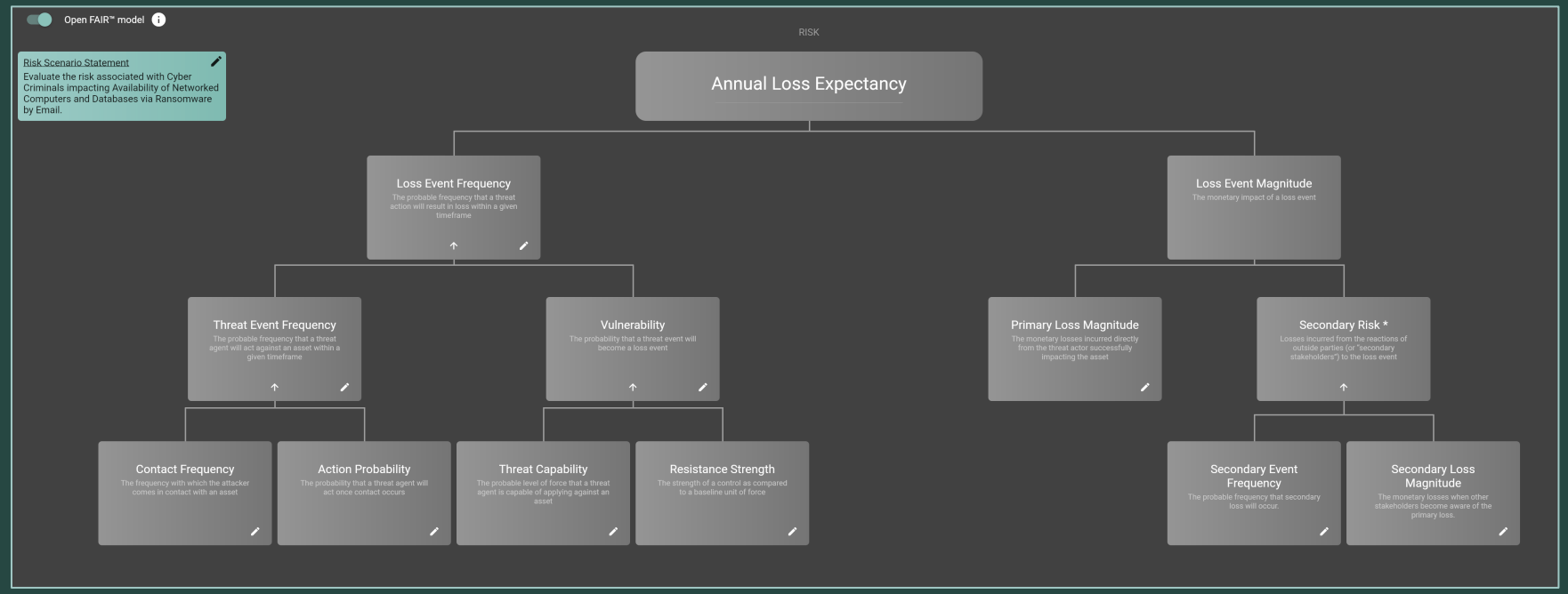
Ostrich Cyber-Risk

END

FORECASTING RISK

VALUE PROPOSITION: ALL FACTORS CONSIDERED

THE PROBABLE FUTURE FREQUENCY AND PROBABLE FUTURE MAGNITUDE OF LOSS RESULTING FROM VARIABLE FACTORS TODAY



BEST USE OF KNOWLEDGE AND DATA AVAILABLE TO REDUCE UNCERTAINTY & **IMPROVE OBJECTIVITY**

CRQ helps you identify and describe why risk drivers MAY be of concern

WHAT ARE WE WORRIED ABOUT?

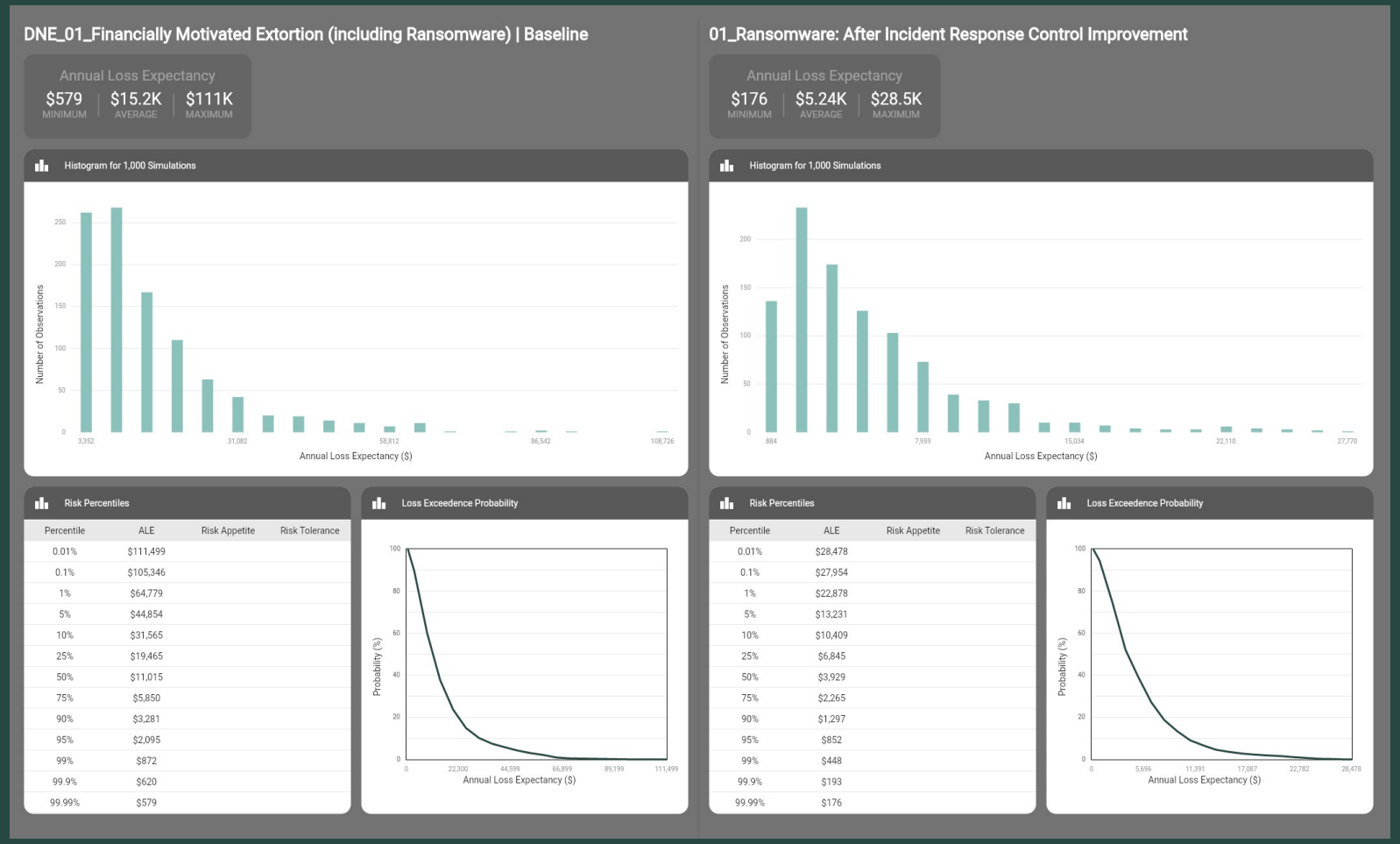
Ostrich Cyber-Risk

THESE ARE NOT MEASUREABLE OR ACTIONABLE RISK STATEMENTS

	Threat Communities	Motives	Target Criteria	Initial Access Vectors	Threat Event	Other TTPs	Exposed Surfaces	Target Assets	Controls	Loss Events	Costs
Ransomware		”Risk”									
Phishing				“Risk”							
Perimeter Risk									”Risk”		
Cloud Vuln Scanning								“Risk”			
Identities									“Risk”		
MFA									”Risk"		

FORECASTING RISK

WHAT SHOULD WE DO ABOUT WHAT?



- "Manage Risk to Goals"
- Determine Fit for Purpose Funding
- Evaluate Control Efficacy
- Compare Investment ROR (Return on Risk)
- Evaluate Third Party, Vendor, M&A, etc. Risk
- Evaluate Externalities (e.g. Pandemic) Risk
- Adjust workflow (Assessment Question Selection)
- Identify Risk Drivers and Control Opportunities
- Justify Compensating Controls
- Drive Decision Consensus
- Reduce Rework & Duplication
- Identify Visibility Risk
- Interpreting Metrics

CRQ is exploratory and can be used to support nearly any decision with an element of "risk".

ZB EXAMPLE 1: RANSOMWARE

SCENARIO 1 OF 3

A financially motivated cybercriminal group targets an organization with ransomware. They gain initial access to the network through a spear-phishing email, which an employee unwittingly opens. The attackers then exploit a vulnerability in the organization's web application to escalate their privileges. They proceed to deploy ransomware on the network, encrypting sensitive data and demanding a ransom for decryption. The attack causes business disruption, financial loss, and reputational damage.

Scenario Family:

Threat Community Attack Motives: Financial: Extortion: _All

Threat Communities: Organized Criminals: Ransomware Gangs & Unaffiliated Malicious: _Any

Target Criteria: Sensitive Data

Threat Event Chain: Ransomware encryption

Threat Community Initial Access Vector: Phishing: General

Threat Community Initial Privilege: Some: Credentialed

Targeted Assets: TECHNICAL: Computers and servers; CONTENT: CORP SENSITIVE; CONTENT: CUSTOMER SENSITIVE

Threat Events/Actions on Objectives: Data: Availability: Encrypt

Vulnerable/Exposed Surfaces: MISCONFIG: OS; KNOWN VULNS: Application; COMMON WEAKNESSES: Lack of Input Validation;

Controls: Anomalies and Events (DE.AE); Protective Technology (PR.PT)

Loss Scenario:

Security and Business Stakeholders: Customers; Employees; Financial Institutions, Market, Insurance Companies

Business Outcomes: AVAILABILITY: DATA: Data not available to Operations; AVAILABILITY: FUNCTION: Business interruption or downtime

Stakeholder Expectations: Reliable and efficient technology systems; Protection of proprietary information; Safe and secure technology systems

Loss Chains: Failure to properly manage contracts and agreements; Inadequate emergency response planning

Cost Drivers: Capital Expense Increase; Revenue: Current Change; Spend to Recover; Spend to Replace

Scenario 2: The same financially motivated cybercriminal group from Scenario 1 uses a watering hole attack to gain initial access. The attackers compromise a website frequently visited by the organization's employees, and when employees visit the site, their devices become infected. The attackers then use the devices to move laterally within the network, deploying ransomware that encrypts critical systems and data. The organization suffers business disruption, financial loss, and reputational damage.

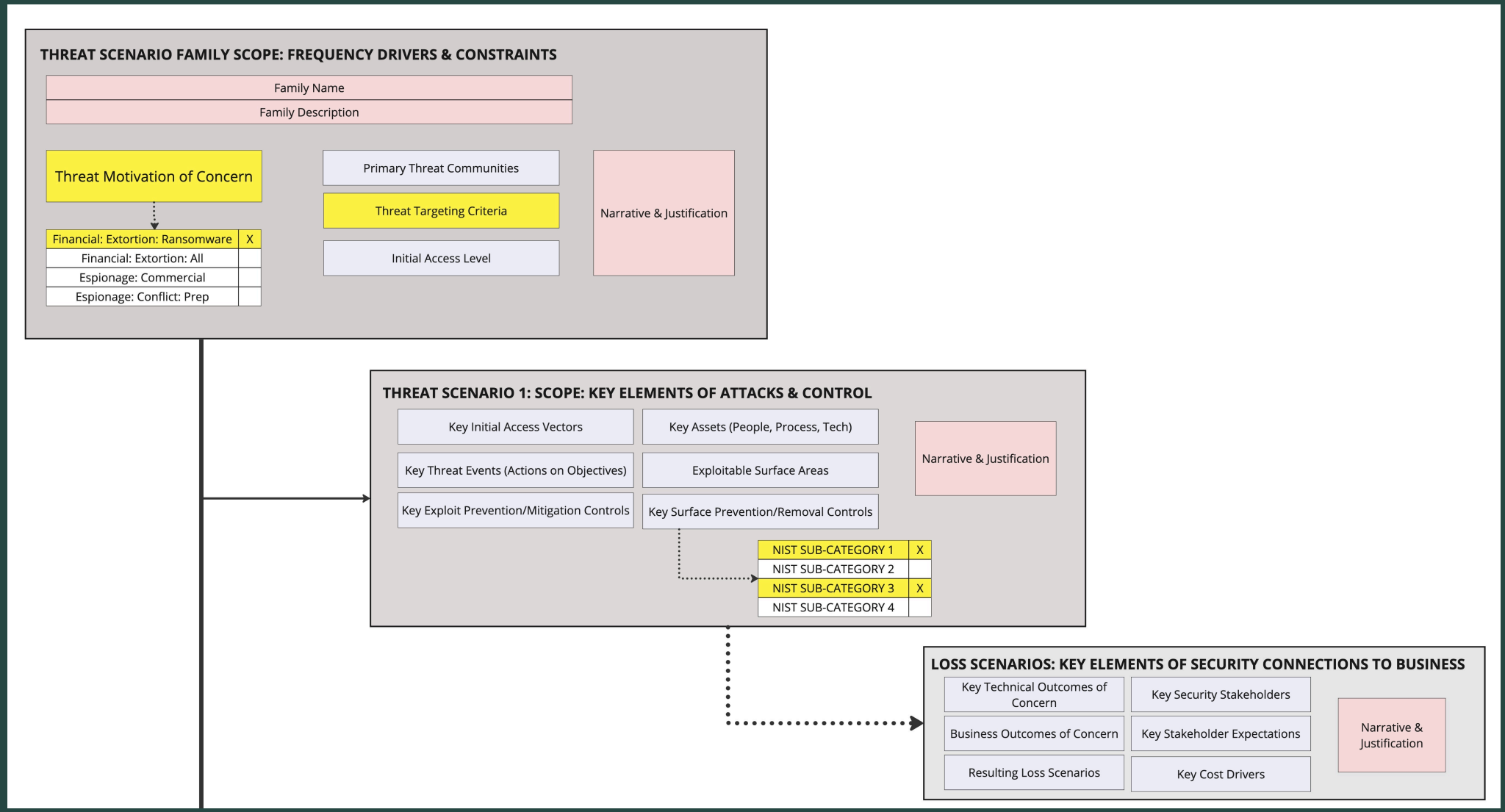
Scenario 3: In this scenario, the same cybercriminal group as in the previous scenarios targets an organization, but with a different approach. They gain initial access to the network through a supply chain attack, compromising a third-party vendor's systems. The attackers then leverage this access to infiltrate the targeted organization's network. Once inside, they deploy ransomware, but instead of encrypting the data, they steal sensitive information and threaten to release it publicly unless a ransom is paid. The organization faces potential reputational damage, financial loss, and legal consequences.

- Identify the main dimensions of the risk scenario (e.g., threat actors, attack vectors, assets, etc.)

- Break down each dimension into smaller, measurable units (e.g., number of threat actors, frequency of attacks, asset values, etc.)

- Establish relationships between units across dimensions to create a holistic view of the risk scenario
- Data
- Etc

ADVANCED SCENARIO SCOPE MANAGEMENT



TOPICS

CRQ DECISION SUPPORT METHODOLOGY

QUALITY METRICS		
KPIs for CRQ Program, Initiative, or Analysis	Compliance	
	Alignment	
	Consensus	
	Integration	
	Application: Use Breadth and Fit	
	Availability	
	Transparency	
	Efficiency	

CONTEXT MANAGEMENT			Models & Assumptions	Information In/Out	Processes / Methods	Tools	RACI & Metrics	GUIDANCE
Core Context Component ("LEGO") Identification and Documentation		People, Processes, Technologies						This is scope information you will need to re-use over time. Maintain currency as able.
		Business Loss Scenarios						
		Security Equities						
		Threat Families						
		Surface & TTP Classes						
		Control Classes						
		Decision Sets (for Measurement Plans)						
		Stressor Sets						
Decision Support Planning	Content Requirements	Topical Breadth and Depth						Think of the decisions you will be supporting. You'll want one measurement plan for every set of decisions needing new output. Try and consolidate and standardize. BASELINE Decision Requirements gathered ANNUALLY - Faster is unsustainable (?)
	Decision Modeling	Question Modeling						
		Decision Criteria						
Measurement Planning	Scenario Family Selection	Threat Motive						These anchor your work over time, allow input data re-use, assure scenarios are thematically stackable, etc - they will not change much. Review annually, but avoid changing unless absolutely required.
		Threat Communities						
		Target Criteria						
	Scenario Flow & Scope Development (Dimensions & Units)	Attack Chains						Attack Chains, Control Chains, Loss Chains, etc. are all detailed "examples" of Scenario Families constructed to make risk measurable. Your BASELINE assumptions here should be reviewed annually, but your comparative and one-off scenario formulations may need out of cycle work - just remember to keep "current version" baseline separate from custom or out of cycle. Roll out-of cycle work here into baseline annually if it needs to be re-used. If you structure this work appropriately, it can be kept in pieces (ie loss scenarios, threat scenarios, sets of controls that work together to accomplish a common objective, etc) NOTE: THIS ALLOWS YOU TO KEEP RELATIVELY STATIC DATA SOURCES OF RECORD EVEN AS YOUR MEASUREMENT PLAN AND DELIVERY REQUIREMENTS CHANGE. This is because if you re-use the same scenario component, you can assume the scope is the same. The smaller the component (eg attack chain), the more likely that scope will match a future requirement. This RARELY happens with "Complete FAIR Scenarios? It's also worth mentioning that A COMPLETE SET OF WELL THOUGHT OUT SCENARIOS CAN ASSURE PRE-DEVELOPMENT OF THE CORE COMPONENTS AND DATA NECESSARY TO QUANTIFY NEARLY ANYTHING with much lower effort and much higher quality,
		TTPs, Surfaces, Controls						
		Loss Chains						
	Stressor & Variance Modeling (Stocks and Flows)	Scenario Variables						
		Variable Change Drivers						
		Change Indicactors						
	Data Source of Record Selector	Requirements						
		Available Option Selection						
		Best Fit Heuristics Applied						

CRQ OPERATIONS			Models & Assumptions	Information In/Out	Processes / Methods	Tools	RACI	GUIDANCE
Measurement Execution	Data Collection / Receipt	Automated/Scheduled						In a perfect world, "Risk Data Requirements" should be developed annually and delivered to agreed on data-provisioning sources of record who will provide you new or updated answers to the same questions/requirements every quarter (for BASELINE cadence), but manual estimates are sometimes needed and validation turns up errors. A solid measurement plan will make this is repeatable and painless as possible.
		Manual Input Estimation						
		Validation						
	FAIR Factor Estimation	Frequency						Even with the best data in the world, forecasts are estimates. There is always some amount of human touch and subjectivity. Try and re-use the came roles every time an estimate is made. Consider standing up an estimation committee and calibrating them.
		Susceptibility						
		Loss						
	Estimation Application	Update Existing Data						Straightforward. Enter estimates into Ostrich Birdseye CRQ
		Enter New Data						
		Simulate						
		QA Results						

DECISION SUPPORT			Models & Assumptions	Information In/Out	Processes / Methods	Tools	RACI	GUIDANCE
Reporting	Baseline Risk	Total						Your BASELINE reporting not only provides your "All Else Being Equal" risk forecast, it also provides the starting point for any Comparative Risk Analysis. Further, it assures you have robust set of components (built in the measurement planning and operations phases) to have a reasonably advanced starting point for any unplanned analysis work. As mentioned earlier, gather data quarterly for this and publish quarterly. You need version control of this because if everyone is operating off of a different forecast, they're making decisions with different assumptions and this breaks operations. It's the same reason we version control software.
		By Scenario						
		By Theme						
	Comparative Risk	Residual						Pre-plan this work if possible. Identify recurring decisions needing comparative reporting. I identify which key factors will need to vary, and why, and develop repeatable heuristics for varying them so that your comparative work is always consistent and transparent. Vary from the Baselines for "How much more / less than expected" or to start off "Option A" and "Option B" in those cases. If this is not pre-planned, review annually for incorporation into planning
		Future						
		A/B Comparison						
	One-Off	Formally Out of Scope						Just what it says.
		New-new in-scope						
		Testing / Theorizing						
Decision Application	Results Analysis	Amounts						This is all about appetites, tolerances, and decision criteria. Consider using GQIM as an aid. Make assumptions about decision-makers where they are unwilling or unable to provide input. This phase should close the loop with and match up to "Decision Support Planning" in context management
		Causes						
	Governance Applied	Decision Options						
		Decision Threshold (eg Tolerance)						

Ostrich Cyber-Risk

END

CRQ: Systematic Analysis, Measurement, & Decision Support

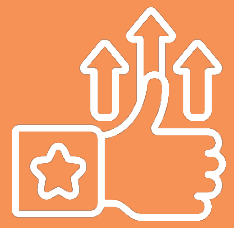
Ostrich Cyber-Risk

1. What are our concerns?

- **Risk Drivers:**
  - Threat Events (Causes)
  - Loss Events (Effects)
  - Specific Uncertainties
- **Risk Questions & Decisions:**
  - Themes (Breadth)
  - Precision (Depth)
  - Appetite & Decision Criteria

2. Why are they concerns?

- **What might play out?**
  - TTPs?
  - Vulnerable Surfaces?
  - **Control Objectives?**
  - Control Availability?
- **Uncertainty (Min, Max, Most Likely)**
  - Frequency / Magnitude
  - Susceptibility (Vulnerability)



5. VISIBILITY?

Where tasks are difficult to complete, this is evidence of "visibility" risk and indicates that your organization may be making decisions without sufficient insight into its risks. **Consider documenting and acting on remediating these gaps as a form of risk reduction**.

3. How much risk?

- **Benchmark: "Similar Classes"**
- **Triage: Calibrated Estimation**
- **Evidence: Data & Metrics** say what?
- **Math** (E.g. **Monte-Carlo**)

4. How should we respond?

- **Loss Manifestation**
  - **Average Exposure** over time
  - **Probability of exceeding** / year
- **Risk Factor Analysis**
  - Frequency vs Magnitude
  - Min vs Max vs Most Likely

The process of CRQ largely consists of the same analytical steps that should have been occurring already

Cyber Risk Quantification:

Better Risk Management through Applied Measurement

Ostrich Cyber-Risk

You were going to make the same decisions with:

1. The same data
2. Less reliable processes
3. More uncommunicated assumptions
4. Incomplete / Discordant models
5. Additional subjectivity
6. Unarticulated uncertainty

CRQ Improves Risk Decisions:

1. Communicability & Tangibility
2. Confidence & Transparency
3. Quality & Outcomes
4. Objectivity & Defensibility
5. Consensus & Acceptance
6. Hidden Ops Costs of “Scores”

Where should CRQ be applied?

Ostrich Cyber-Risk

1. Objectives of CRQ

- Develop Consensus
- Provide & normalize risk objectives
- Make better decisions than before
- Quantify & Communicate confidence and uncertainty

2. CRQ & Complexity

- CRQ does not complicate cyber risk management
- Instead, it increases precision and identifies gaps in risk visibility
- You were already going to make a decision with the same information

3. When to Implement CRQ

- For high-stakes decisions
- Where decisions have unclear criteria
- Where consistency is vital for success
- When there is a fragmented context
- When there is difficulty achieving consensus

4. Making CRQ useable

- Not every aspect demands the same level of thoroughness
- Take advantage of “ranges” and “samples”
- Decide what information is needed to govern ahead of time
- Quantification of qualitative inputs is accepted science
- The process and math improve what you already know

POTENTIAL “RISKS” FROM TRADITIONAL APPROACHES

- Decision Quality: Improper or incomplete risk factor assessment
- Ops Efficiency: Prioritizing poorly doesn’t reduce work
- Uncertainty: Lack of confidence/assurance awareness limits agility

Ostrich Cyber-Risk

END OF MAYBE