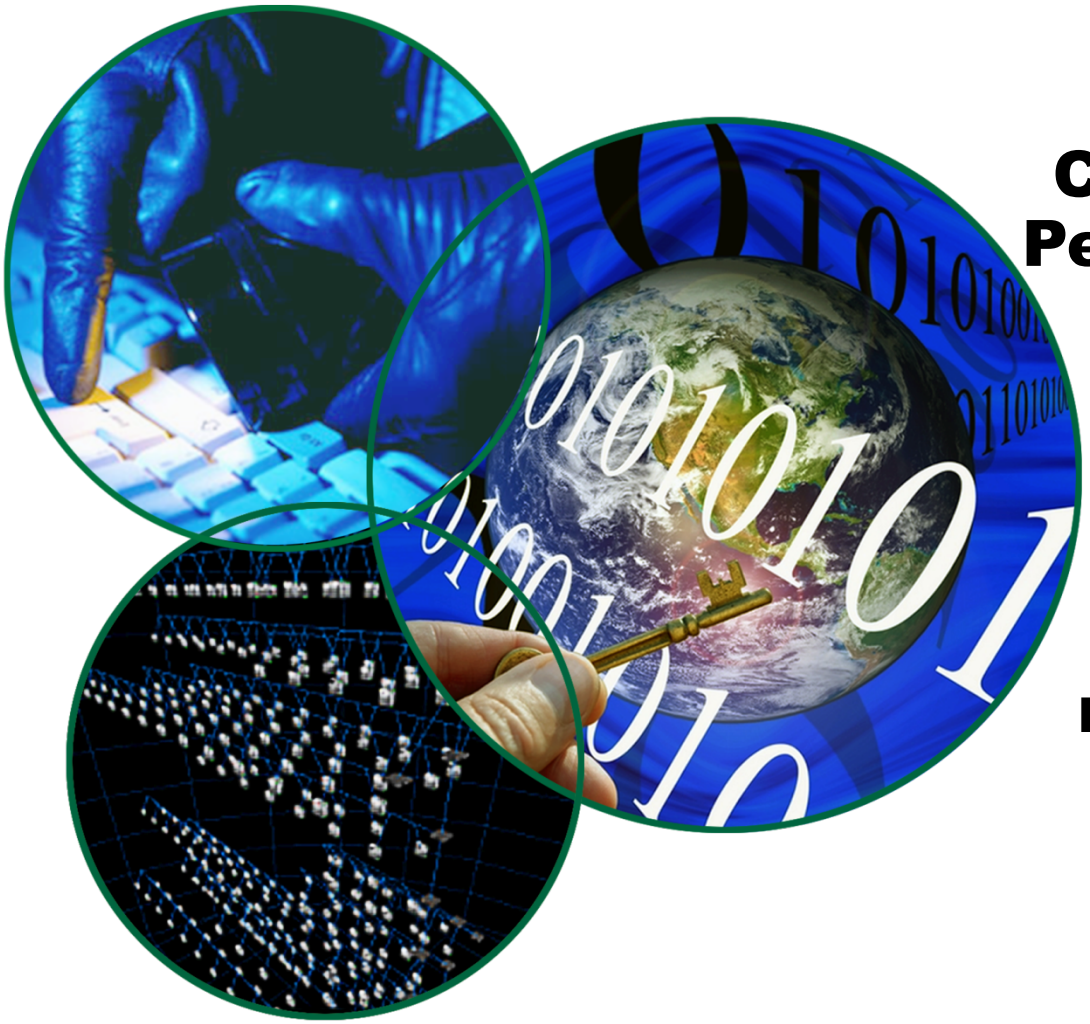
Oak Ridge National Laboratory:
Delivering 21st Century Science and Technology



Evaluating Security Controls Based on Key Performance Indicators and Stakeholder Mission

Frederick T. Sheldon, Ph.D.

Robert K. Abercrombie, Ph.D.

Ali Mili, Ph.D.

June 11, 2009

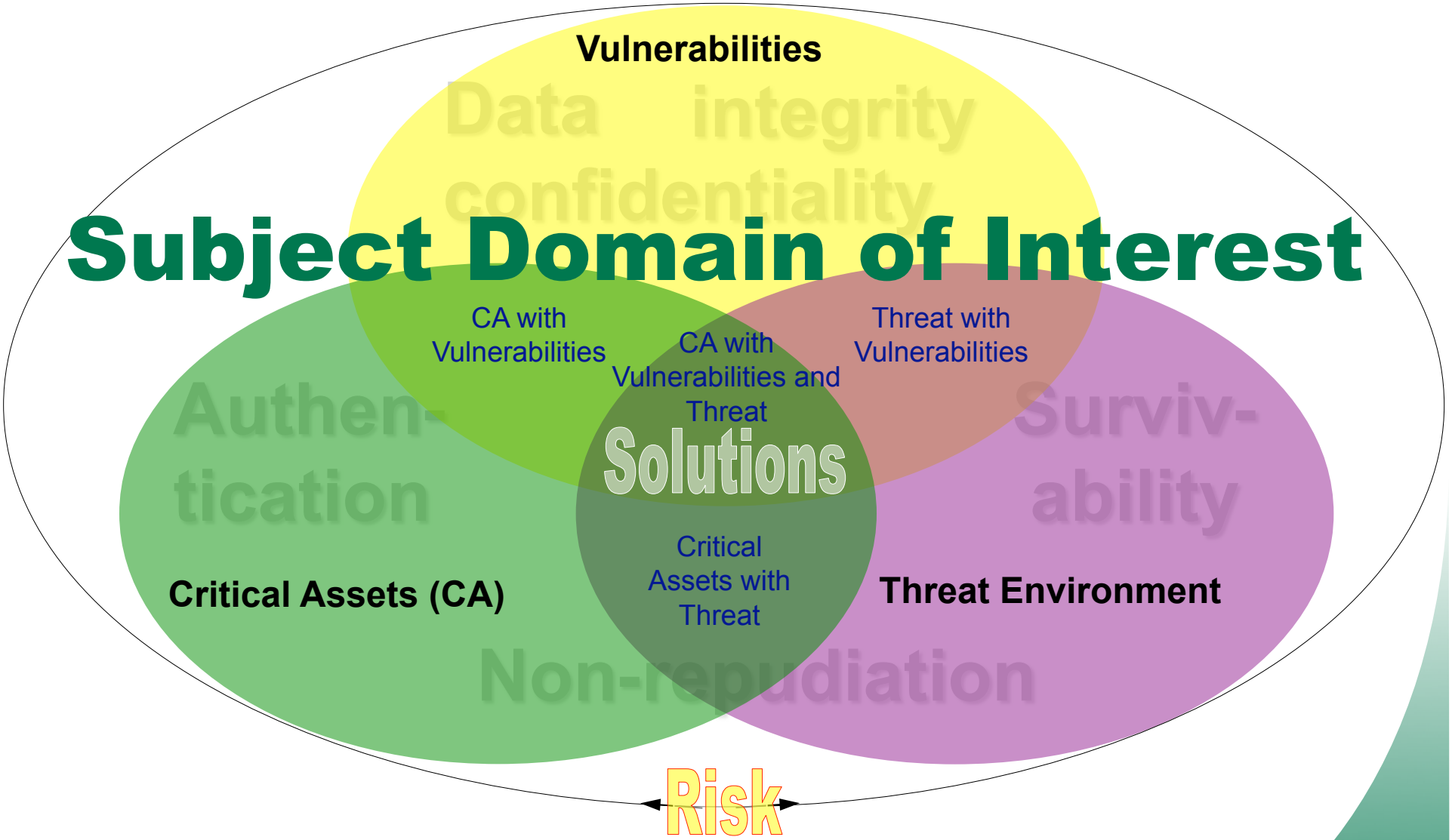
Managed by UT-Battelle
for the Department of Energy

The submitted manuscript has been authored by a contractor of the U.S. Government under contract DE-AC05-00OR22725. Accordingly, the U.S. Government retains a nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or allow others to do so, for U.S. Government purposes.

Oak Ridge National Laboratory

Today's Agenda

- **The Subject Domain of Interest:**
  - **Cyberspace Dominant Infrastructures**
- **The Need:**
  - **The Security Gap: A Looming Crisis**
- **The Approach:**
  - **What is needed for *disciplined security management***
- **One Enabling Technology:**
  - **Cyber Security Econometrics System**
    - **Process**
    - **Impact**


Vulnerabilities
Data integrity
confidentiality
Subject Domain of Interest
CA with Vulnerabilities
CA with Vulnerabilities and Threat
Threat with Vulnerabilities
Authen-tication
Solutions
Surviv-ability
Critical Assets with Threat
Critical Assets (CA)
Threat Environment
Non-repudiation
Risk

The Security Gap: A Looming Crisis

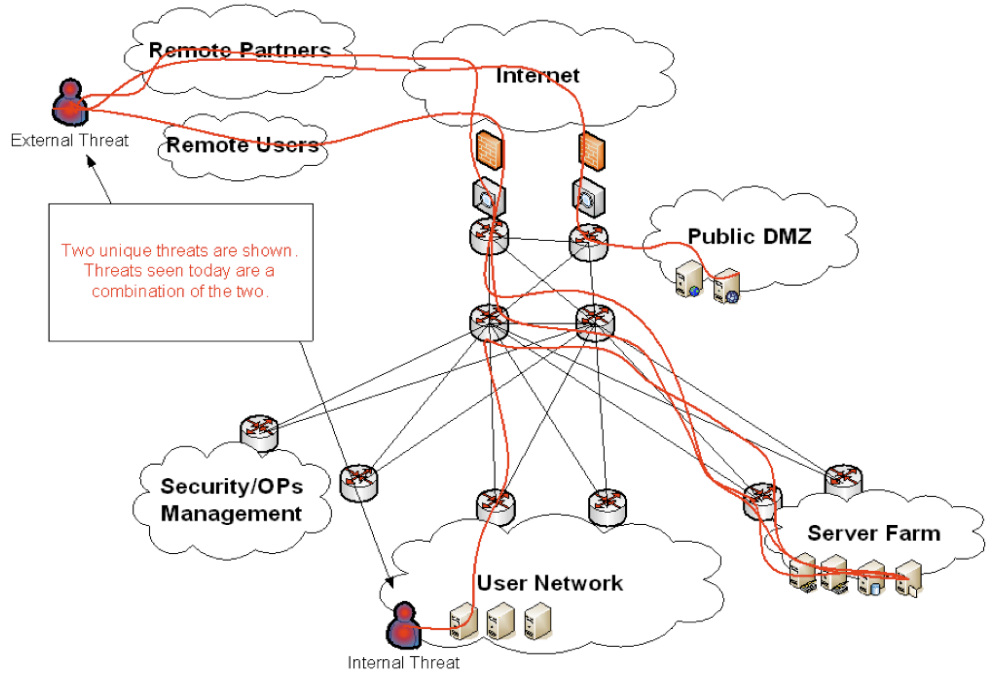
- **Increased threat**
  - as a consequence of:
    - emerging global tensions and
    - increased sophistication of the perpetrators
- **Increased criticality**
  - because the emergence of the Internet has shifted more economic and social activity online, making security virtually synonymous with cyber security
- **Increased vulnerability**
  - because emerging computing paradigms such as
    - networking,
    - distributed computing, and
    - mobile/pervasive computing

  open wide security gaps that are hard to control

What is needed for *disciplined security management*

- **A logic**
  - for specifying security requirements and verifying secure systems against such requirements.
- **A model**
  - for managing system security by quantifying
    - costs,
    - risks, and
    - measures/countermeasures
  - for estimating ROI.
- **Automated tools**
  - that support security management according to the proposed models.

CSE Rationale



- **Consistent with the spirit of *Value Based Software Engineering* and comprehends the different organizational mission needs for all stakeholders.**
  - **For example, CSE identifies information assurance controls and mitigation costs as an investment toward assuring mission success, including**
    - **Essential activities such as real-time threat analysis and**
    - **Fed by knowledge discovery tools and capabilities within the threat and vulnerability space.**
- **Framework enables us to rapidly develop new metrics that offer a bottom line understanding of the costs and benefits of alternative approaches to securing cyberspace assets.**

Cyber Security has many dimensions

- Focused on either the left or right side of boom (i.e., a significant event)
  - left side are preemptive/protective measures including all steps prior to the "system's" deployment
  - right side includes damage assessment and recovery measures
- CSES is designed to enable comprehensive exploration of the "likely" consequences of the various trade-offs.
- Consider a general example

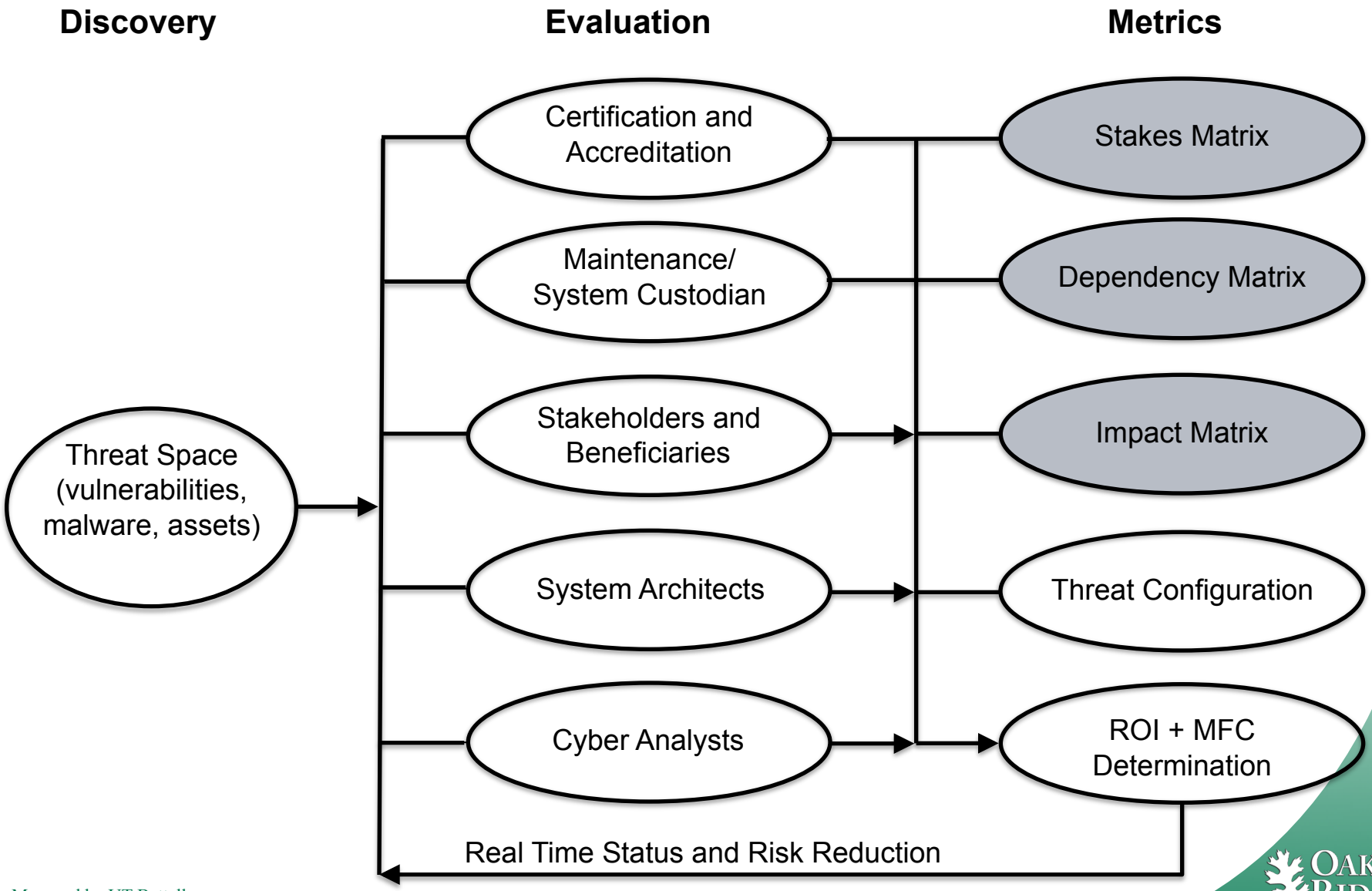
Oak Ridge National Laboratory

CSES general example

- Identify vulnerabilities and provide options to mitigate these vulnerabilities at their earliest stages before they become more pernicious
- Codify the concomitant methodologies and processes that consider the full range of stakes (criticality/assets) and associated (operational) risks, and
- Manage explicit investments such as countermeasures, certification and accreditation (C&A) among the many feasible left side courses of action.
- Ultimately, as the system evolves the precision (and accuracy) of the assessments will help all aspects from C&A, intrusion avoidance, attribution including such measures as return on investment (ROI) and mean failure cost (MFC).

Oak Ridge National Laboratory

Process of discovery, evaluation/measurement and metrics computation and generation



Oak Ridge National Laboratory

Process of CSES follows:

- **Determination of:**
  - **Stakes Matrix**
  - **Dependency Matrix**
  - **Impact (Threat) Matrix**
  - **Mitigation Costs Matrix**
- **Allows for Application of CSES by:**
  - **Online Security Monitoring**
  - **Charging Verification & Mitigation Costs**
  - **Integrating Quality Costs**

Stakes Matrix: Stakeholders vs. Requirements

- **Premises necessary for MFC estimation:**
  - **A stakeholder may have different stakes in different requirements**
  - **A requirement may carry different stakes for different stakeholders**
- **Best represented with 2 dimensional matrix**

		Requirements				
		R_1	R_2	R_3	…	R_n
Stakeholders	S_1					
	S_2					
	S_3					
	…				$FC_{i,j}$	
	S_m					

cost that stakeholder S_i would lose if the system failed to meet requirement R_j

$$MFC(S_i) = \sum_{R_j} FC_{i,j} \times P(R_j)$$

Probability that the system fails to meet requirement R_j

Oak Ridge National Laboratory

Stakes Matrix: Stakeholder vs. Requirements

		Security Requirements				
		R1	R2	R3	…	Rn
Stakeholders	S1					
	S2					
	S3					
	…				FC_i^j	
	Sm					

The Stakes Matrix showing how Failure Cost (FC) is derived.

The estimation of mean failure cost depends on the following premises:

- The same stakeholder may have different stakes in different security requirements.
- The same security requirement may carry different stakes for different stakeholders.

The best way to represent this situation is through a 2 dimensional matrix, where the rows represent stakeholders, the columns represent security requirements, and the entries represent stakes, as shown below in the Table.

The FC entry at row i, column j, represents the cost that stakeholder Si would lose if the system failed to meet the security requirement Rj (i.e., also represented as FC(Si,Rj)).

Stakeholder	•Requirements	
	•Requirement 1: Safety record	•Requirement 2: Timeliness
Passengers	•Personal Safety	•Convenience, Scheduling
Airline company	•Liability for Loss of Life •Reputation of airline	•Reputation with for timeliness / Public relations
Aircraft Manufacturer	•Liability for Loss of Life •Reputation of aircraft	•Zero
Accident Insurance of Aircraft	•Premium owed for loss of aircraft	•Zero
Life Insurance of Passenger	•Value of life insurance	•Zero

Dependency Matrix: Requirements vs. Components

		Components					
		C_1	C_2	C_3	…	C_k	C_{k+1}
Requirements	R_1						
	R_2						
	R_3						
	…				$\pi(R_i\|E_j)$		
	R_n						

- **Links the probability of failing a particular requirement with the probability of failure of a component of the system**
- **Simplifying hypothesis: assume that violations affect no more than one component at a time**
- **Let E_i, for $1 \le i \le k$, be the event: failure of component C_i**
  - **Event E_{k+1}: no component has failed**

Probability of failing requirement R_i given component C_j fails

Probability of requirement R_i failing

Probability of component C_j failing

$$P(R_i) = \sum_{j=1}^{k+1} \pi(R_i|E_j) \times \pi(E_j)$$

Oak Ridge National Laboratory

Dependency Matrix: Requirements and Components

		Components				
		C1	C2	C3	…	Ck
Requirements	R1					
	R2					
	R3					
	…				$\pi(R_i \mid E_j)$	
	Rn					

- An analysis of the system architecture, by architecture subject matter experts, can lead to the derivation of conditional probabilities that link the probability of component failures with the probabilities of failing to meet specific requirements.
- This information can be represented in a 2 dimensional matrix, which we call the **Dependency matrix**.
- The term π(Ej) represents the probability of event Ej
- The term π(R|Ej) represents the probability of failing to satisfy requirement Ri, given hypothesis Ej (i.e., that event j has occurred).
- In the table there exists a component event Ej for a requirement Ri where the probability of failure to satisfy requirement R exists (π (Ri|Ej)):

Components Requirements	Processing Components	Login Component	Secure Storage Component	User Profile Analysis
Freedom from Insider Threats	0.01	0.6	0.2	0.98
Protection of Critical Data	0.01	0.2	0.98	0.2
Access Control	0.01	0.98	0.4	0.1

The *Dependency* Matrix showing the relationship between Requirements and their distinct respective components and failure results (probability) with Respect to Passenger.

Impact Matrix: Component Failure vs. Threats

		Threats					
		T_1	T_2	T_3	…	T_h	T_{h+1}
Components	C_1						
	C_2						
	C_3						
	…				$\pi(E_i\|V_j)$		
	C_k						
	C_{k+1}						

- **To assess the likelihood of a particular threat leads to failure of a component:**
  - **Set of threats $T_1, T_2, \ldots, T_h$**
  - ***Events* $V_1, V_2, \ldots, V_h, V_{h+1}$**
  - **V_i, $1 \le i \le h$: Threat *i* has materialized**
  - **V_{h+1}: No threat *i* has materialized**
  - **Assume that no more than one threat materializes at a time**

Probability of component C_i failing given threat T_j materializing

Probability of component C_j failing

Probability of threat T_j materializing

$$\pi(E_i) = \sum_{j=1}^{h+1} \pi(E_i|V_j) \times \pi(V_j)$$

Oak Ridge National Laboratory

Impact Matrix (Component Failure vs Threat Relationship)

		Threats				
		T1	T2	T3	…	Th
Components	C1					
	C2					
	C3					
	…				$\pi(E_i \mid V_j)$	
	Ck					

The *Impact* Matrix showing Component Failure versus Threats Relationship Grouping

- To assess the likelihood that a particular threat leads to the failure of a component, we consider a set of cataloged threats (or families of threats with common attributes), say T1, T2, T3, … Th, and we consider the events V1, V2, V3, … Vh, Vh+1, where Vi, for $1 \le i \le h$, stands for: Threat i has materialized, and Vh+1 stands for: No threat i has materialized.
- The probability of threat Tj (which is π(Vj)) to the probability of component failure for component Ci (which is π(Ei)). To apply this formula, we need to derive the conditional probabilities, which we propose to represent in a 2 dimensional matrix, that we call the ***Impact* matrix**.

Components	Threats				
	Insider Threats	Intrusions	Denial of Service Threats	Authentication Threats	No Threat
Processing Component	0.2	0.4	0.8	0.8	0.0
Login Component	0.2	0.2	0.2	0.2	0.0
Secure Storage Component	0.2	0.4	0.2	0.2	0.0
User Profile Analysis	0.2	0.1	0.1	0.1	0.0

Summary of Calculation of MFC

$$Y_i = \sum_{i \le j \le m} X^j \times A_i^j, 1 \le i \le n$$

Y: vector of size n
A: n×m matrix
X: vector of size m

$$Y = A \circ X$$

$$MFC(S_i) = \sum_{R_j} FC_{i,j} \times P(R_j)$$

ST: Stakes Matrix
PR: vector of requirement failure probabilities

$$MFC = ST \circ PR$$

$$P(R_i) = \sum_{j=1}^{k+1} \pi(R_i|E_j) \times \pi(E_j)$$

DP: Dependency Matrix
PE: vector of component failure probabilities

$$PR = DP \circ PE$$

$$\pi(E_i) = \sum_{j=1}^{h+1} \pi(E_i|V_j) \times \pi(V_j)$$

IM: Impact Matrix
PV: vector of threat emergence probabilities

$$PE = IM \circ PT$$

$$\boxed{MFC = ST \circ DP \circ IM \circ PT}$$

Oak Ridge National Laboratory

Mitigation Costs (MC) Matrix

		Components							
		C1	C2	C3	C4	C5			
Requirement Fulfilled or Service Delivered	S1							Verification Cost by Service	VS1
	S2								VS2
	S3								VS3
	S4			D_i^j					VS4
	S5								VS5
		Verification Cost by Component							
		VC1	VC2	VC3	VC4	VC5			

- Each requirement fulfilled or service delivered by the system depends on the correct operation of one or more system components.
- This dependency can be quantified by the statistical correlation between the failure of the component and the failure to deliver the service or fulfill the requirement.
- If we combine this dependency with the cost of verifying each component of the system, we can maintain an estimate of the probabilities of service delivery (discussed above) as a function of the effort invested in enhancing the dependability of the individual components. Maintaining this information can serve two purposes:
  - First, to determine, at all times, which components must be enhanced first to improve overall stakeholder satisfaction.
  - Second, to charge verification costs according to stakeholder benefit. For any particular verification measure, we charge stakeholders according to the gains they have achieved as a result of this measure (which are quantified by the reduction of their mean failure cost).
- The verification cost by service can be estimated by the following formula:

$$VS_i = \sum_{i=1}^{n} D_i^j \times VC_j .$$

Oak Ridge National Laboratory

Estimating the Probability of Threats

- Utilizing the previous defined matrices,
  - the ***Stakes matrix*** (ST) is filled by stakeholders according to the stakes they have in satisfying individual requirements;
  - the ***Dependency matrix*** (DP) is filled in by the system architect (i.e., cyber security operations and system administrators) according to how each component contributes to meet each requirement;
  - the ***Impact matrix*** (IM) is filled by analysts according to how each component is affected by each threat.
- The remaining question is how to fill the vector of threat emergences probabilities (PV) that represents the probability of emergence of the various threats that are under consideration?
  - This is done empirically, by simulating and/or operating the system for some length of time and estimating the number of threats that have emerged during that time and continue to be refined as the system evolves.
  - From these numbers, we infer the probability of emergence of all the threats during one hour of operation.
- This results in a vector of mean failure costs of all stakeholders as :

$$MFC = ST \circ DP \circ IM \circ PV.$$

OAK RIDGE National Laboratory

Integrating Quality Costs

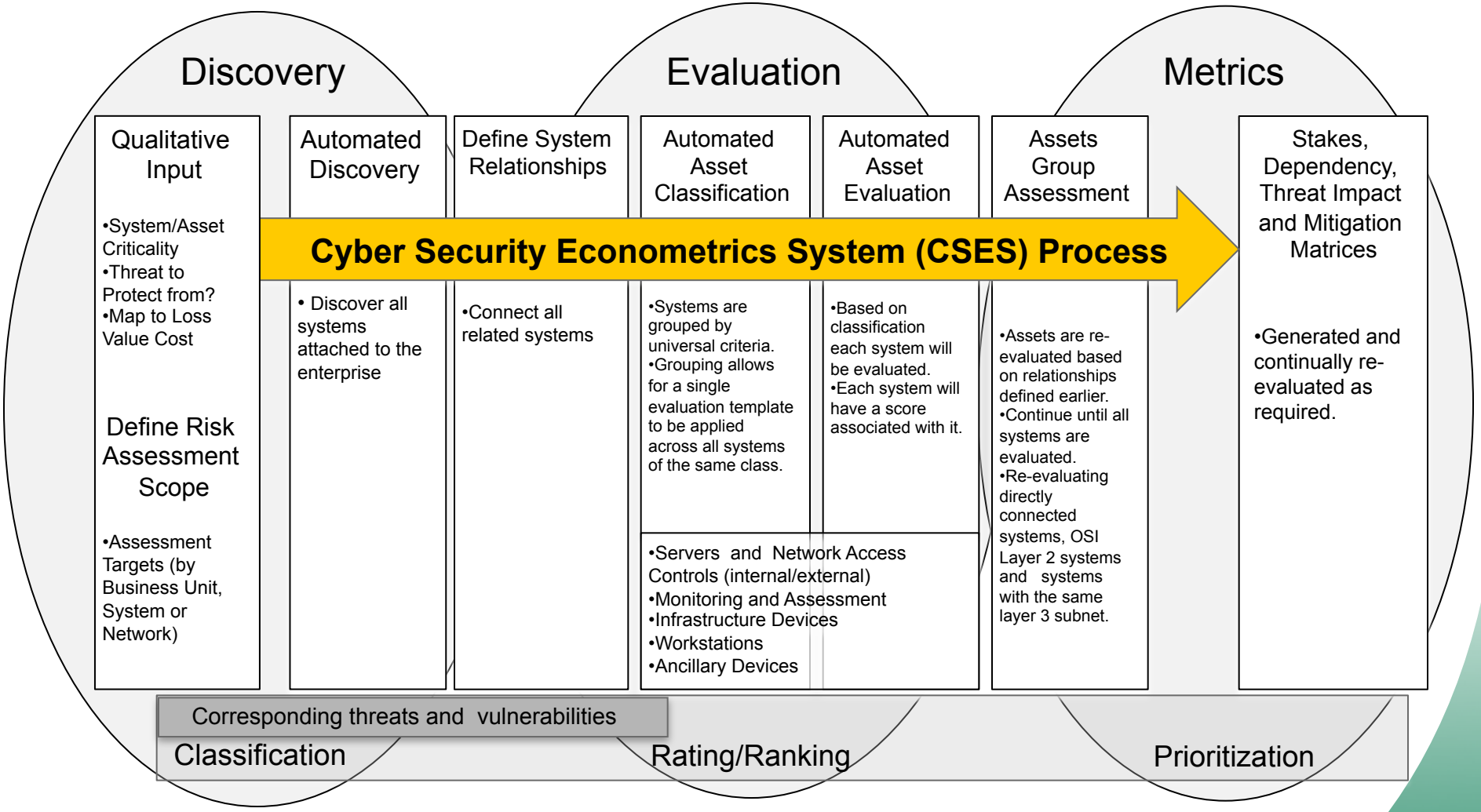
- **From the standpoint of each stakeholder, the mean failure cost (which is the cost we expect to incur as a result of the lack of security) must be balanced against the cost of improving system security. Our mean failure cost model allows us to formulate the tradeoff of quality versus cost in terms of a return on investment equation. Specifically, a return on investment model is defined by the following parameters:**
  - **An initial investment cost, say IC,**
  - **An investment cycle (duration), say T,**
  - **An return over the investment cycle, say B(t), for 1 ≤ t ≤ T, and**
  - **A discount rate, say d.**
- **Then the return on investment is given by the following formula:**

$$ROI = -1 + \sum_{t=1}^{T} \frac{B(t)}{IC \times (1+d)^t}.$$

- **The formula of mitigation costs can be used to compute IC, estimating the benefit gained by Stakeholder *S* during time period *t* by computing the difference between the mean failure cost with the current component and the mean failure cost with a validated component.**

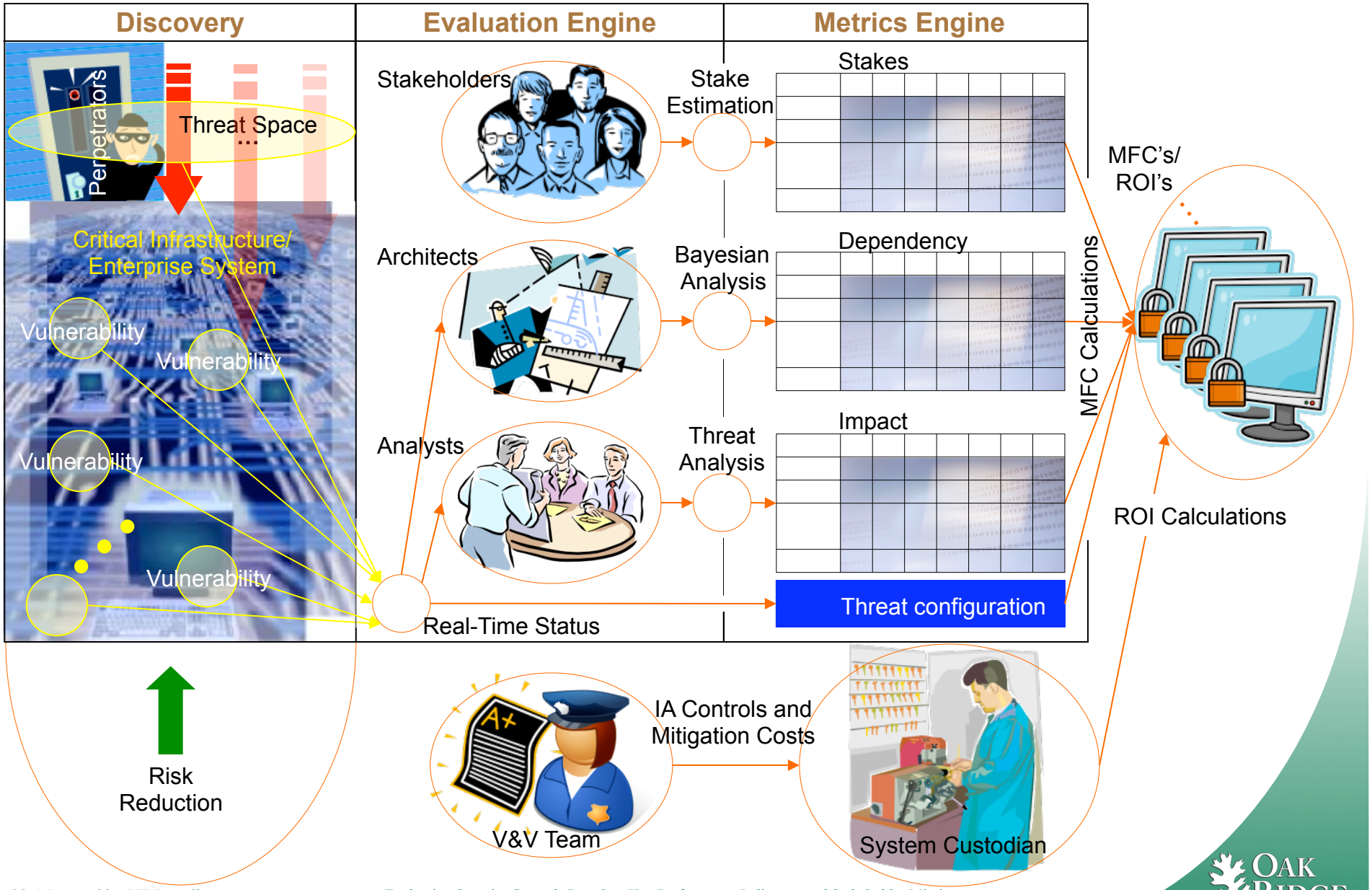
OAK RIDGE National Laboratory

Quantitative Framework for Information Security Risk Management

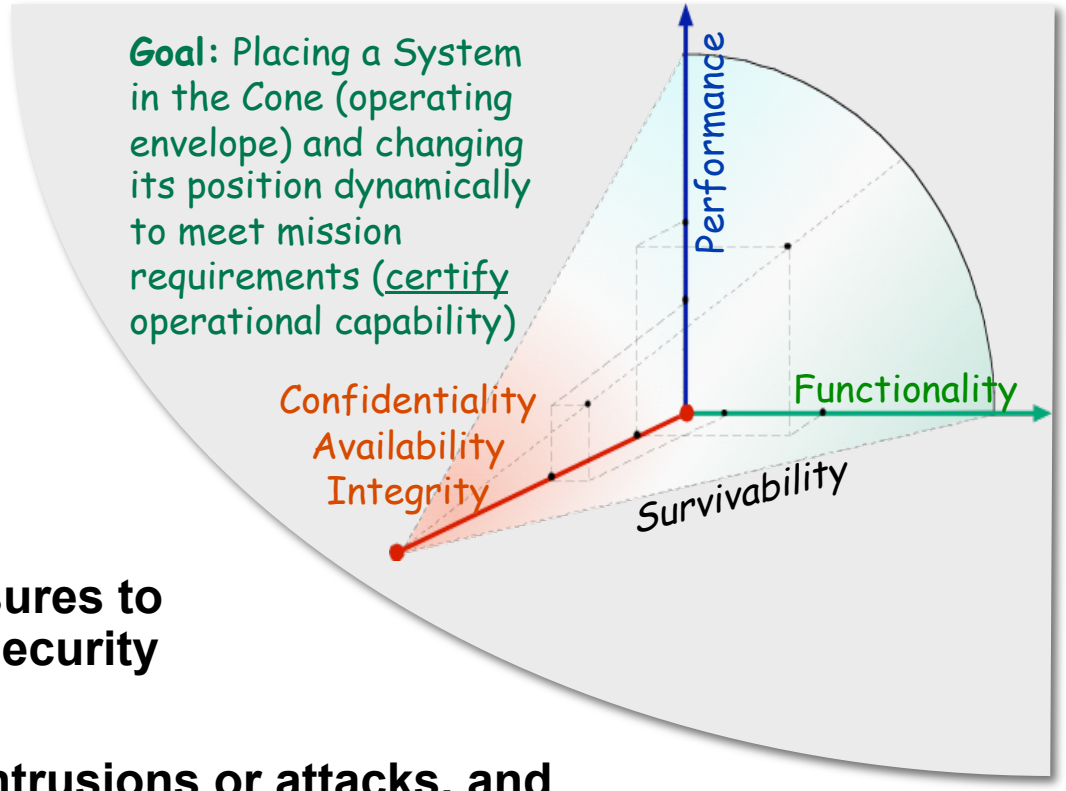


Oak Ridge National Laboratory

Cyber Security Econometrics (CSE)



Conclusions



CSES

- **Provides a framework for measuring the appropriate attributes that support the decisions necessary to:**
  - **Design security countermeasures to choose between alternative security architectures,**
  - **Respond to events such as intrusions or attacks, and**
  - **Improve security (including reliability and safety) during both design and operational phases.**
- **Provides a comprehensive basis for choosing courses of action that have the highest risk reduction return on investment, i.e., reduce the most risks for the lowest cost.**

Future work for CSES that will enable *disciplined security management*

- **We presented:**
  - **A logic**
    - for specifying security requirements and verifying secure systems against such requirements.
  - **A model**
    - for managing system security by quantifying
      - costs,
      - risks,
      - measures/ countermeasures, and
    - for estimating ROI.
- **What is needed (our future proposed work)**
  - **A set of automated tools**
    - that support security management according to the proposed models.
    - that capture the various stakes of distinct stakeholders
  - **A rich set of multilayered security requirements**
    - High level and their derived requirements
  - **A interesting architecture with intertwined security and processing components**
  - **A rich catalog of threats families**
- **Hope to demonstrate effectiveness and practicality of system**

Oak Ridge National Laboratory:
Meeting the challenges of the 21st century

Robert K. Abercrombie, Ph.D., Frederick T. Sheldon, Ph.D., Ali Mili, Ph.D.

Email: abercrombier@ornl.gov, sheldonft@ornl.gov, ali.mili@njit.edu
Phone: (865) 241-6537, (865) 576-1339, (973) 596-5215