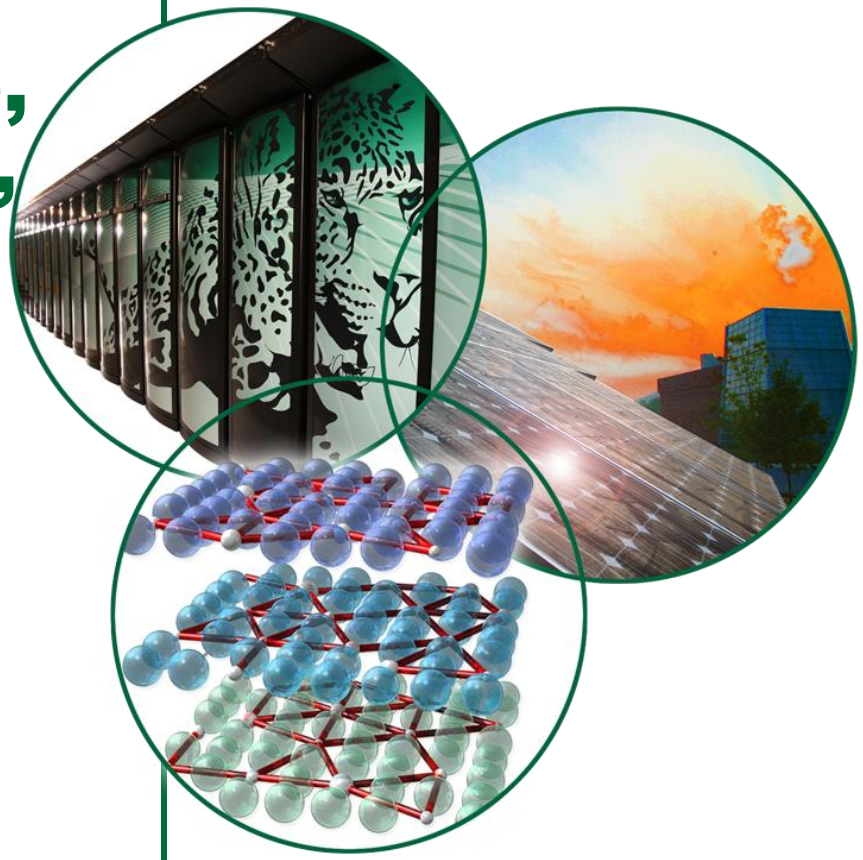
# Identification and Monitoring of Critical Success Factors for Effective e-Commerce, e-Learning, e-Training, and e-Democracy



**Presented at:**

**First International Conference on Electronic Management**

**Tripoli, Libya**

**Robert K. Abercrombie, Ph.D.**

**June 1-3, 2010**

U.S. 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

MANAGED BY UT-BATTELLE FOR THE DEPARTMENT OF ENERGY

# Agenda For Today's Presentation

## Identification and Monitoring of Critical Success Factors

### for Effective e-Commerce, e-Learning, e-Training, and e-Democracy

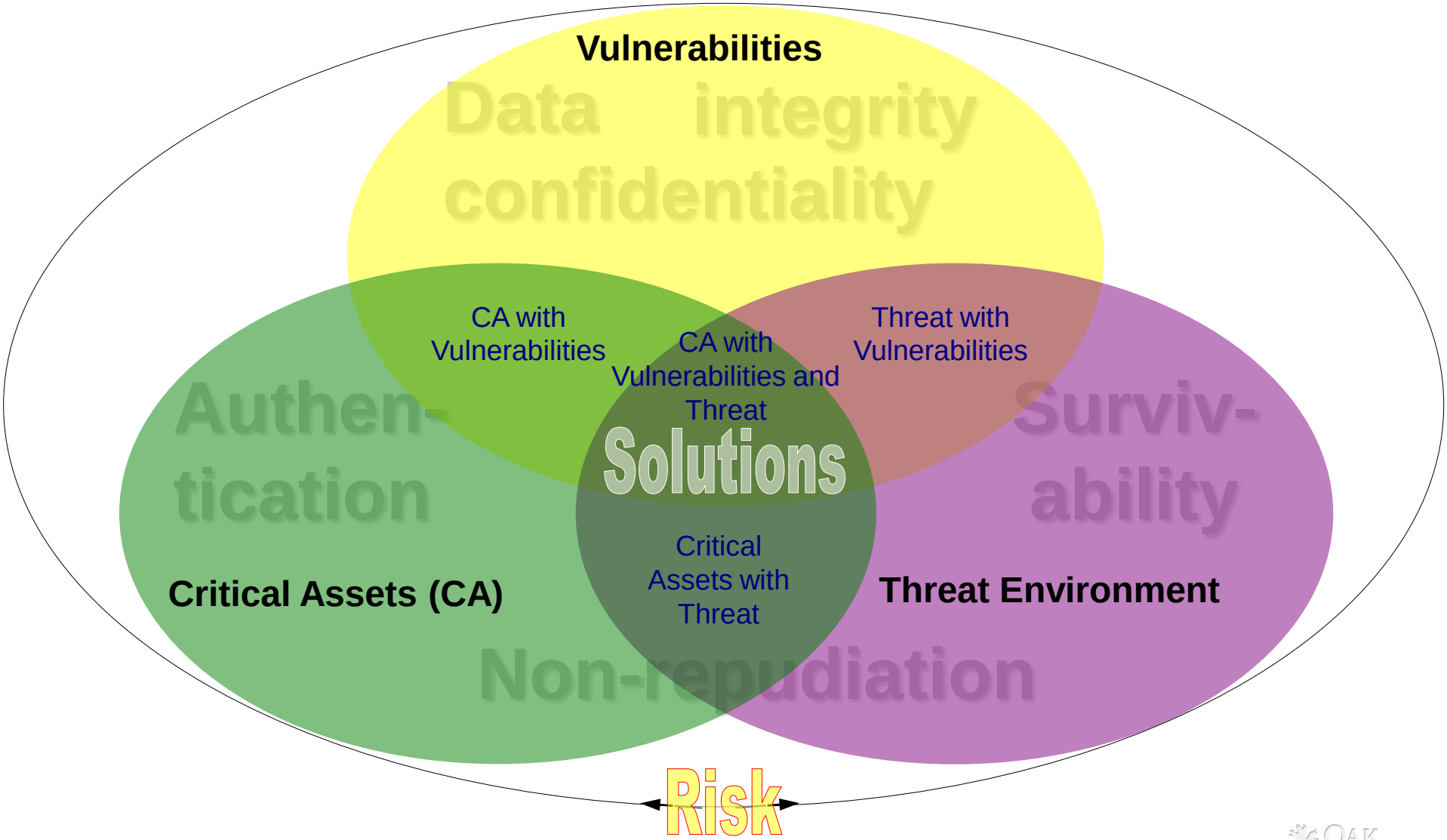
- Background Need
  - The Security Gap: A Looming Crisis: Risk associated with critical assets, vulnerabilities and the threat environment
- A Candidate Disciplined Solution – Our Proposed Approach
  - A logic
  - A model
  - Automated tools
- One Enabling Technology - Expanded Explanation: Application of Mean Failure Cost
  - Stakes Matrix: Stakeholders versus Requirements
  - Dependency Matrix: Requirements versus Components
  - Impact Matrix: Components Failure versus Threats
  - Mitigation Costs Matrix: Verification Costs via Requirements or Components
- Conclusions and Future Directions

# The Security Gap: A Looming Crisis

- Increased threat
  - as a consequence of:
    - reality of global tensions,
    - organized crime, 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

# Background Need
# The Security Gap: A Looming Crisis



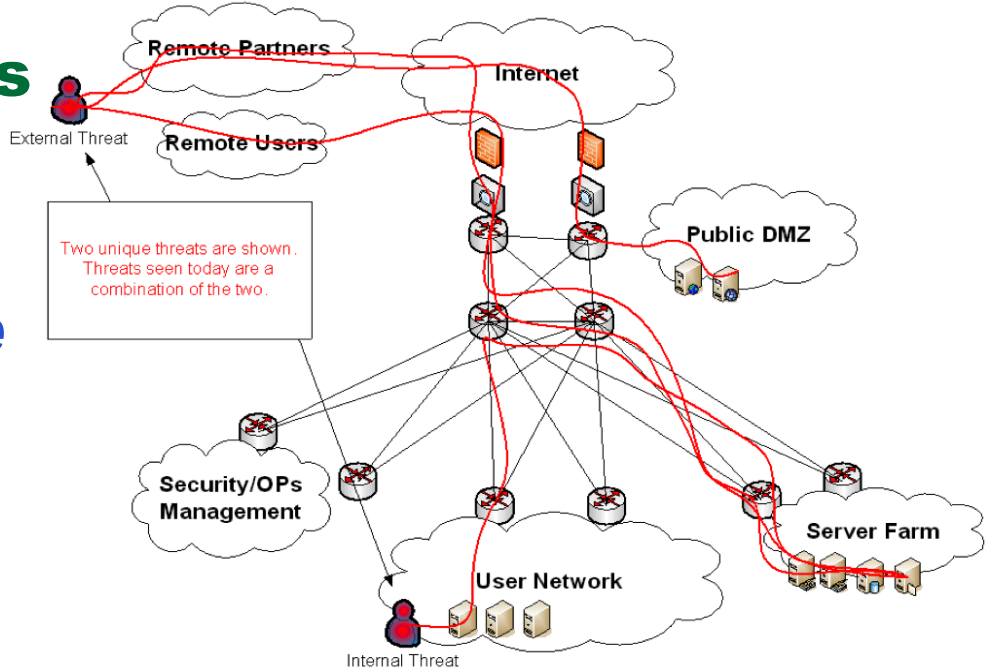
# What is needed for *disciplined security management*

- 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.

# Proposed Automated Tool

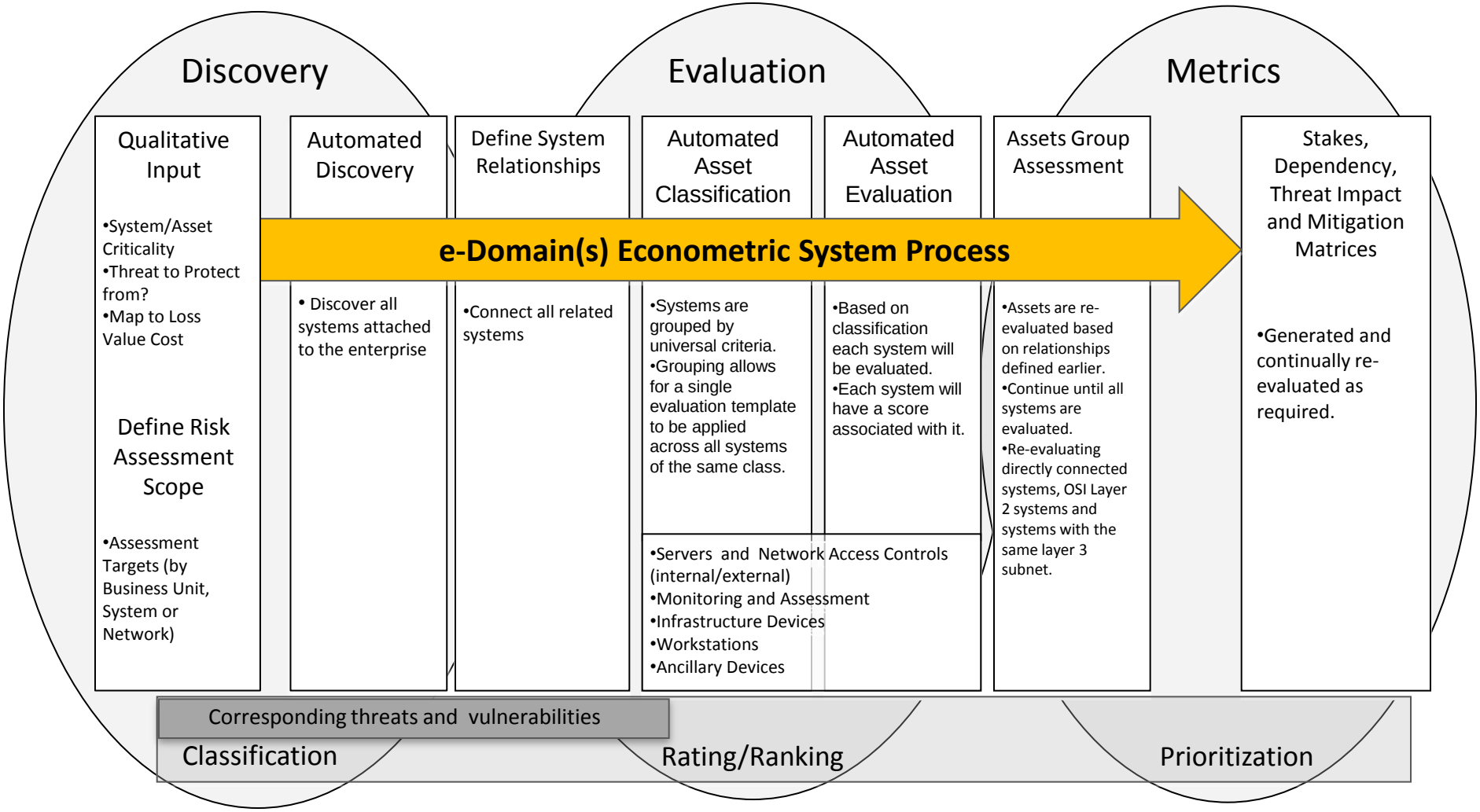
- Automated Tool:
  - Cyber Security Econometrics System (CSES) → eDomain(s) Econometrics System
    - With adaptations for:
      - e-Commerce, e-Learning, e-Training, and e-Democracy
    - Provides a quantitative indication of reliability, performance, and/or safety of a system accounting for the criticality of each requirement as a function of one or more stakeholders' interests in that requirement
    - Provides a comprehensive basis for choosing courses of action that reduce the most risks for the lowest cost
  - Utilizes the concept of Mean Failure Cost (MFC)
    - Reveals how much each stakeholder stands to lose from mission value due to a requirement or component of the system failing
    - Not intrinsic to the system but varies by stakeholder
    - To estimate MFC, initially need:
      - Set of stakeholders, Set of requirements
      - For each stakeholder and each requirement, the stake the stakeholder attaches to the requirement
      - For each component of a requirement, the likelihood that the system provides the service as specified

# e-Domain(s) Econometrics Process Rationale

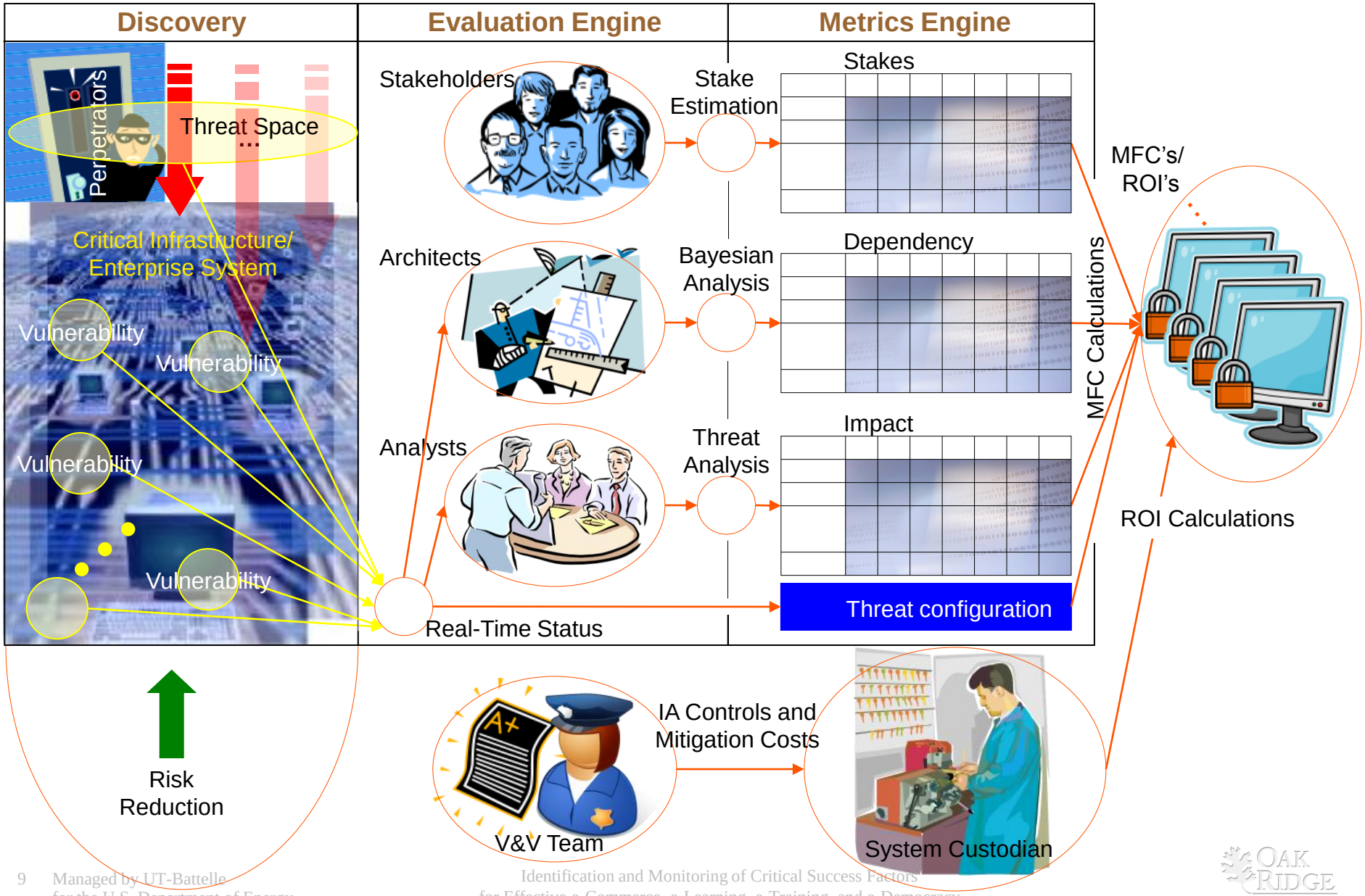



- Consistent with the spirit of *Value Based Software Engineering* and comprehends the different organizational mission needs for all stakeholders.
  - For example, e-Domain(s) Econometrics System identifies information assurance controls and mitigation costs as an investment toward assuring mission 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.

# Quantitative Framework for e-Domain(s) Econometrics



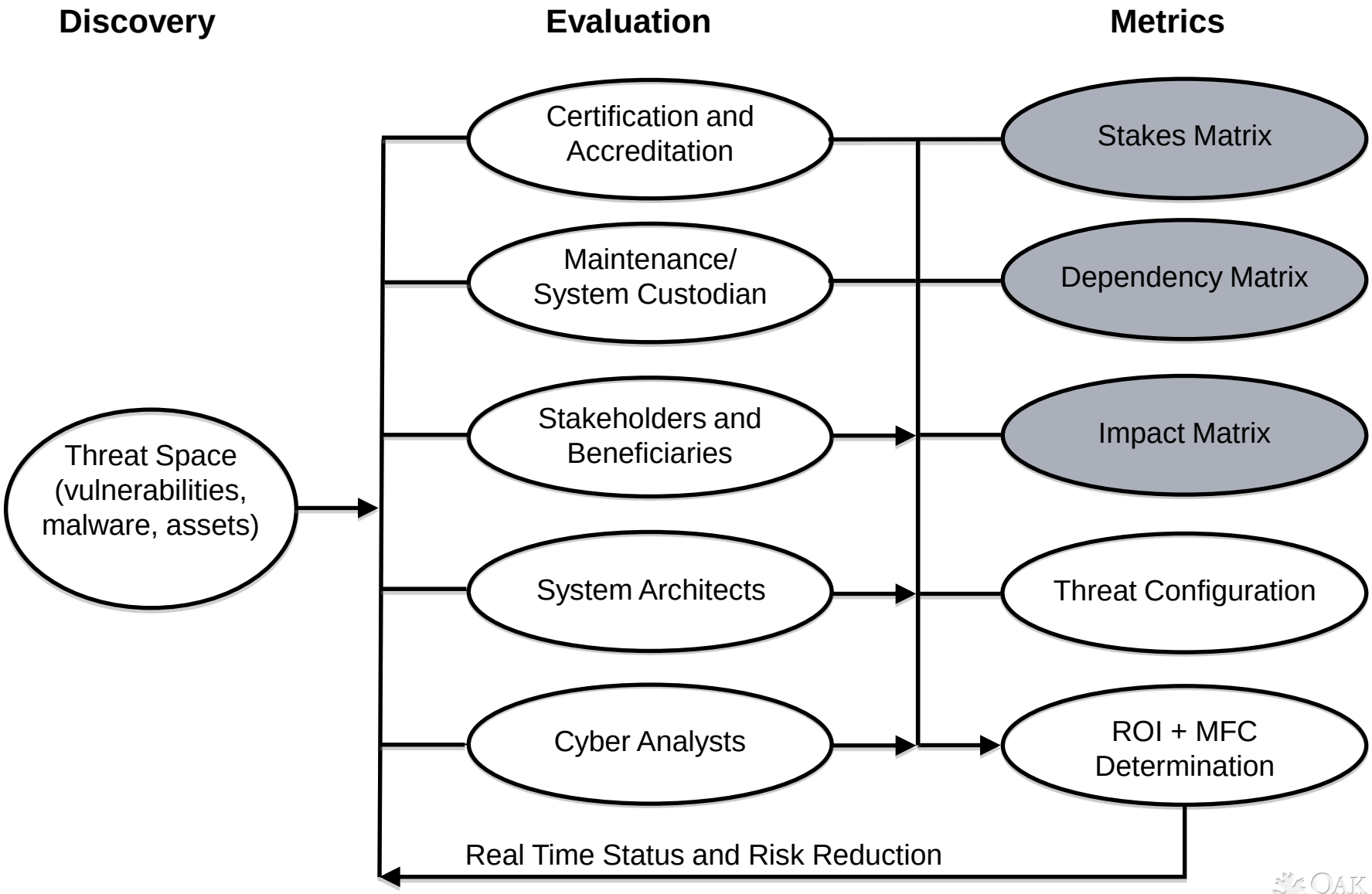
# e-Domain(s) Econometrics System Process



# eDomain(s) Econometric System – A 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).

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



# Process of the Automated Tool

- Determination of:
  - Stakes Matrix by the Stakeholders
  - Dependency Matrix by the Architects
  - Impact (Threat) Matrix by the Verification and Validation (V&V) Group
  - Mitigation Costs Matrix by the Analysts and V&V Group
- Applications Domain Space:
  - e-Commerce, e-Learning, e-Training, and e-Democracy Computing Infrastructure Integrity Establishment
  - e-Commerce, e-Learning, e-Training, and e-Democracy Computing Infrastructure Integrity Monitoring
    - Online security monitoring
    - Charging verification and mitigation costs
    - Manage investments such as countermeasures and certification and accreditation
    - 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:**
  - Rows: Stakeholders
  - Columns: Requirements
  - Entries: Stakes

| | | 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 $R_j$

# *Stakes* Matrix: Stakeholder vs. Requirements

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

The Stakes Matrix below illustrates an example of how Failure Cost (FC) is derived.

The FC entry at row *i*, column *j*, represents:

- the cost that stakeholder $S_i$ would lose if the system failed to meet the security requirement $R_j$.

| Stakeholder | •Requirements | |
|---|---|---|
| | •Requirement 1: Safety record | •Requirement 2: Timeliness |
| **Passengers** | •Personal Safety | •Convenience, Scheduling |
| **Airline company** | •Liability for Loss of Life<br>•Reputation of airline | •Reputation with for timeliness / Public relations |
| **Aircraft Manufacturer** | •Liability for Loss of Life<br>•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 | $R_1$ | | | | | | |
| | $R_2$ | | | | | | |
| | $R_3$ | | | | | | |
| | … | | | | $\pi(R_i \mid E_j)$ | | |
| | $R_n$ | | | | | | |

- **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

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

# *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 $\pi$(Ej) represents the probability of event Ej
- The term $\pi$(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 ($\pi$ (Ri|Ej) ):

| Requirements | Components | | | |
|---|---|---|---|---|
| | 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

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

# *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 $\pi$(Vj)) to the probability of component failure for component Ci (which is $\pi$(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
X: vector of size m
A: n×m matrix

$$Y = A \circ X$$

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

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
PT: vector of threat emergence probabilities

$$PE = IM \circ PT$$

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

# *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 |
| | | | | | | | $VS_i = \sum_{i=1}^{n} D_i^j \times VC_j .$ | |
| | | Verification Cost by Component | | | | | | |
| | | VC1 | VC2 | VC3 | VC4 | VC5 | | |

- Each *requirement fulfilled* or *service delivered* by the system <u>depends</u> 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 as a function of the effort invested in enhancing the dependability of the individual components. Maintaining this information can serve two purposes:
  - Which components must be enhanced first to improve overall stakeholder satisfaction.
  - 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 in MFC).

# 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:

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

# Integrating Quality Costs

- **Stakeholder standpoint: the mean failure cost (i.e., cost we expect to incur as a result from 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 $1 \le t \le T$, 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.**

# eDomain(s) Econometric System – Specific Examples

- Good candidate for a system consists of:
  - Credible and distinct stakeholders
  - Rich requirement structure
  - Non-trivial architecture of components
  - Catalog of families of threats
- Demonstrates effectiveness and practicality of system
  - e-Commerce Example
  - e-Domains Infrastructure Integrity Example
    - Deploying an Anti-Virus
    - Deploying Redundant Servers / Processor

# Taking Cues from Reliability

- **Reliability:**
  - Mean Time Between Failures (MTBF)
  - Mean Time to Failure (MTTF)
- **Security:**
  - Mean Time to Detect (MTTD)
  - Mean Time to Error (MTTE)
- **MTBF, MTTF: Major flaws:**
  - Independence vis-à-vis stakeholders
  - Independence vis-à-vis requirements clauses
  - Independence vis-à-vis Verification & Validation Measure

# The Mean Failure Cost

- **Summary Formula from:**

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

- **Stakes matrix, ST: Stakeholders.**
- **Dependability matrix, DP: architects.**
- **Impact matrix, IM: V&V group.**
- **Threat vector, PT: Security team.**

# e-Commerce Example

## Security Requirements:

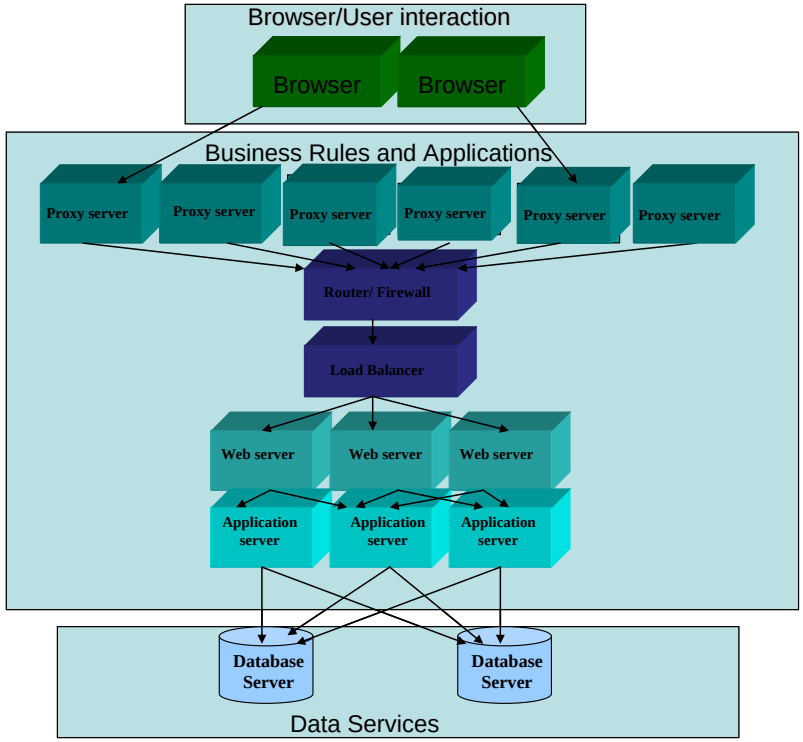
- Confidentiality: data only available to those authorized
- Integrity: information has not been altered by unauthorized parties
- Availability: application is operational when needed
- Non-repudiation: no party in a transaction can deny participation
- Authenticity: all parties are properly authenticated with appropriate privileges and responsibilities
- Privacy: user information is not improperly disclosed

Stakes Matrix: Cost of failing a security requirement in $/hour

| | | Security Requirements | | | | | |
|---|---|---|---|---|---|---|---|
| | | Conf | Int | Avail | Non-rep | Auth | Priv |
| Stakeholders | Customer | 10 | 5 | 3 | 4 | 6 | 12 |
| | Merchant | 120 | 70 | 140 | 110 | 105 | 6 |
| | Technical Intermediary | 20 | 20 | 40 | 20 | 30 | 20 |
| | Financial Intermediary | 20 | 60 | 50 | 40 | 40 | 60 |

# Dependency Matrix:

| | | Components | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Browser | Proxy Server | Router/ Firewall | Load Balancer | Web Server | Application Server | Database Server | No Failure |
| Security | Conf | 0.2 | 0.2 | 1.0 | 1.0 | 0.333 | 0.333 | 0.5 | 0.0 |
| | Int | 0.2 | 0.2 | 1.0 | 1.0 | 0.333 | 0.333 | 0.0 | 0.0 |
| | Avail | 1.0 | 1.0 | 1.0 | 1.0 | 0.333 | 0.333 | 0.0 | 0.0 |
| | Non-rep | 0.2 | 0.2 | 1.0 | 1.0 | 0.333 | 0.333 | 0.0 | 0.0 |
| | Auth | 0.2 | 0.2 | 1.0 | 1.0 | 0.333 | 0.333 | 0.5 | 0.0 |
| | Priv | 0.2 | 0.2 | 1.0 | 1.0 | 0.333 | 0.333 | 0.5 | 0.0 |



## Threats:

- Threats on communication protocols (Comm)
- Threats on the systems and the standard applications (Sys)
- Threats on the information (Info)
- Passive listening (List)
- Virus
- Trojan horse (Troj)
- Denial-of-service or distributed denial-of-service (DoS)
- Threats on the database (DB)

## Impact Matrix:

| | | Threats | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | Comm | Sys | Info | List | Virus | Troj | DoS | DB | NoT |
| Components | Brwsr | 0.0 | 0.1 | 0.1 | 0.1 | 0.3 | 0.4 | 0.2 | 0.0 | 0.0 |
| | PS | 0.5 | 0.1 | 0.1 | 0.3 | 0.3 | 0.4 | 0.2 | 0.0 | 0.0 |
| | R/FW | 0.5 | 0.1 | 0.1 | 0.3 | 0.3 | 0.4 | 0.6 | 0.0 | 0.0 |
| | LB | 0.0 | 0.1 | 0.1 | 0.1 | 0.3 | 0.4 | 0.6 | 0.0 | 0.0 |
| | WS | 0.0 | 0.6 | 0.6 | 0.2 | 0.3 | 0.4 | 0.2 | 0.0 | 0.0 |
| | AS | 0.0 | 0.1 | 0.1 | 0.1 | 0.3 | 0.4 | 0.2 | 0.0 | 0.0 |
| | DBS | 0.0 | 0.1 | 0.1 | 0.0 | 0.5 | 0.6 | 0.3 | 0.8 | 0.0 |
| | NoF | 0.4 | 0.3 | 0.1 | 0.1 | 0.05 | 0.05 | 0.1 | 0.2 | 1.0 |

# Threat Configuration:

| | | Probability |
|---|---|---|
| Threats | Comm | 0.01 |
| | Sys | 0.02 |
| | Info | 0.01 |
| | List | 0.01 |
| | Virus | 0.03 |
| | Troj | 0.06 |
| | DoS | 0.03 |
| | DB | 0.02 |
| | NoT | 0.81 |

# Calculated Mean Failure Cost:

| Stakeholders | MFC ($/hour) |
|---|---|
| Customer | 8.11 |
| Merchant | 112.97 |
| Technical Intermediary | 31.18 |
| Financial Intermediary | 54.24 |

# Security Measures Synopsis

- Tentative classification into five categories:
  - Mitigation measures:  controlling the stakes matrix
  - Failure Tolerance measures:  controlling the dependability matrix
  - Fault Tolerance Measures: controlling the impact matrix
  - Evasive Measures:  Controlling the Threat Vector

# Assessing Security Measures and Security Impact - Process

- We want to improve the security of the system by taking some measures. Question: how do we know if the measure is worthwhile? How do we dispatch the cost of the measure on different stakeholders?
  - We propose: Computing its ROI.
    - Investment cycle length, Discount rate, Investment cost, Episodic (e.g. yearly) costs/ benefits
    - Estimating the yearly benefits of the security measure:
      - Computing the current MFC, hypothetical MFC if the measure is implemented.
      - Computing the MFC difference, in $/Hr.
      - Converting it to $/yr using hours of usage per year for each stakeholder.
- How do we dispatch investment costs on stakeholders?
  - In proportion to MFC gains,
  - In such a way as to make ROI's equal across stakeholders.
- Is the investment worthwhile?
  - For each stakeholder: if ROI>0,
  - For the community: according to community-wide formula of benefit (NPV's are additive, ROI's are not).

# e-Domains Infrastructure Integrity Example

## Comparison of two specific examples comparing Individual ROI versus Enterprise ROI

- Deploying an Anti-Virus System

| Stakeholders | Inv. Cost | Stakeholder ROI | Enterprise ROI |
|---|---|---|---|
| Customer | $0.98 | -0.98 | 0.073 |
| Merchant | $1,426.36 | 0.118 | 0.073 |
| Tech. Int. | $391.98 | 0.114 | 0.073 |
| Financial Int. | $680.68 | 0.111 | 0.073 |
| | $2,500.00 | | |

- Deploying Redundant Servers / Processors

| Stakeholders | Inv. Cost | Stakeholder ROI | Enterprise ROI |
|---|---|---|---|
| Customer | $39.21 | -0.934 | 4.216 |
| Merchant | $45,377.49 | 4.4077 | 4.216 |
| Tech. Int. | $12,351.18 | 4.3348 | 4.216 |
| Financial Int. | $22,232.12 | 4.5183 | 4.216 |
| | $80 000.00 | | |

# Conclusions and Future Directions

- Proposed metric of Mean Failure Cost (MFC) used in examples quantifies stakeholder value of requirements in $/hr of operation can be expanded to all facets of e-Domains.
- Can be used to make effective economics-based decision making for identifying and monitoring critical success factors, as described by stakeholders for effective:
  - e-Commerce, e-Learning, e-Training, and e-Democracy

# References


- A. Ben Aissa, A. Mili, R. K. Abercrombie, and F. T. Sheldon, "Modeling Stakeholder/Value Dependency through Mean Failure Cost," *Proceedings of 6th Annual Cyber Security and Information Intelligence Research Workshop (CSIIRW-2010),* ACM International Conference Proceeding Series, Oak Ridge, TN April 21-23, 2010.
- A. Ben Aissa, A. Mili, F. T. Sheldon, and R. K. Abercrombie, "Software Requirements for a System to Compute Mean Failure Cost," *Proceedings of 6th Annual Cyber Security and Information Intelligence Research Workshop (CSIIRW-2010),* ACM International Conference Proceedings Series, Oak Ridge, TN April 21-23, 2010.
- Anis Ben Aissa, Robert K. Abercrombie, Frederick. T. Sheldon, and Ali Mili, "Quantifying Security Threats and Their Potential Impact: A Case Study," in *Innovation in Systems and Software Engineering: A NASA journal*, in press, 2010.
- F. T. Sheldon, R. K. Abercrombie, and A. Mili, "Methodology for Evaluating Security Controls Based on Key Performance Indicators and Stakeholder Mission," *IEEE Proceedings of the 42nd Annual Hawaii International Conference on System Sciences (HICSS-42), (CD-ROM)*, Waikoloa, Big Island, Hawaii, January 5-8, 2009, Computer Society Press, 2009 (10 pages).
- R. K. Abercrombie, F. T. Sheldon, and A. Mili, "Synopsis of Evaluating Security Controls Based on Key Performance Indicators and Stakeholder Mission Value," in *11th IEEE High Assurance Systems Engineering Symposium (HASE '08),* Nanjing, China, 2008, pp. 479-482.
- F. T. Sheldon, R. K. Abercrombie, and A. Mili, "Evaluating Security Controls Based on Key Performance Indicators and Stakeholder Mission," *Proceedings of 4th Annual Cyber Security and Information Intelligence Research Workshop - Theme: Developing Strategies to Meet the Cyber Security and Information Intelligence Challenges Ahead*, ACM International Conference Proceeding Series, Vol. 288, Oak Ridge, TN, May 14, 2008.

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

Robert K. Abercrombie, Ph.D.
Email: abercrombier@ornl.gov
U.S. Phone: +1 (865) 241-6537
http://www.csiir.ornl.gov/abercrombie