

Research Synopsis

Resource Allocation in Business Information Technology Infrastructure

This project applies risk and consequence assessment models to the IT infrastructure of a corporate environment to evaluate risks and investigate optimal countermeasure resource allocation from a business perspective.

Modeling Area: Risk Management

Case Studies Supported: Resource Allocation

Principal Investigator: Jeffrey L. Duffany

Institution: Universidad del Turabo

Other Investigators: Terry Benzel(USC/ISI), Charles Meister(USC/MSB/ICIP), Morley Winograd (CTM).

Brief Description:

The purpose of this research is to apply risk and economic assessment methodologies to the IT infrastructure of a corporate environment. This study will quantify the various candidate threats and the economic impacts of these threats. The model will be applicable to the study of the cumulative effect of many small events, the impact of large single events, or a small number of medium sized events. A small event would be for example the theft of a laptop computer or a virus affecting an individual computer or IT infrastructure component. A large scale event would be a denial of service attack or the theft or destruction of critical financial information or intellectual property. The economic impact of these threats on the corporation will be then be assessed, enabling cost-benefit analysis of the impact of countermeasures. Countermeasures will be then be modeled in terms of the cost of implementation and the associated risk mitigation factor. Optimization methods will then be applied to determine countermeasure resource allocation.

Objectives:

This research will develop risk assessment and risk management models for the information infrastructure in a corporate environment. This model will provide a methodology which can be adapted to broad range of situations and used to guide decision makers regarding the risk-based

Resource allocation

Infrastructure vulnerability

Threat frequency

Business consequences

resource
allocation

allocation of funding for countermeasures against threats to corporate information infrastructure. This will yield a model that can be applied in different contexts to reflect different factors such as cyber-terrorism and natural disasters. A second goal of developing this model is to use it for corporate executive training through the Institute for Critical Information Infrastructure Protection (ICIIP) at the USC/Marshall School of Business (MSB), USC/ISI (Information Sciences Institute) and CTM (Center for Telecommunications Management).

Interfaces to other Center Projects: This work will leverage work done by Vicki Bier and Luca Quadrifoglio in the area of optimal resource allocation.

Interfaces to non-Center Projects: This work will maintain a close interface with ICIIP/MSB (Charles Meister), USC/ISI (Terry Benzel) and USC/CTM (Morley Winograd).

Major Products and Customers:

Project deliverables will consist of a report that will: (a) develop one or more comprehensive methodologies for risk-based resource allocation among countermeasures to threats against information infrastructure in a corporate environment. Customers: Corporate/industry IT professionals, DHS (b) provide material for a professional short course for corporate clients such as Lockheed–Martin. Customers: ISI and ICIIP (c) Provide a new case study that can be used by CREATE researchers and also applied to other contexts such as cyberterrorism and natural disasters. Customers: DHS and CREATE researchers. (d) Research publications and reports. Customers: general public, DHS, CREATE, ICIIP, ISI, CTM, other university researchers.

Technical Approach:

The methods developed will build on previous research for risk assessment and economic impact and will rely on mathematical programming for optimal resource allocation. Consequence assessment models and risk reduction assessments will be based on a mix of methodologies including probabilistic risk analysis, economic analysis and qualitative assessments. Methods for combining these assessments will be grounded in the theory and methods of multiattribute utility and value models. The overall resource allocation framework uses mathematical programming including linear and nonlinear programming.

Major Milestones and Dates:

1. Week 1: Meet with team members to set goals and objectives, conduct background research.
2. Week 2: Investigate resources available at CREATE and ISI in terms of software and databases. Define problem in mathematical or other appropriate terms. Develop several possible solution approaches.
3. Week 3: Define several candidate business IT topologies and infrastructures. Discuss solution approaches with team members.
4. Week 4: Gather statistics on top threats and vulnerabilities to specific IT components. Develop generate preliminary results based on one or more methods.
5. Week 5: Develop threat scenarios and economic business consequence of each. Continue generating preliminary results making modifications to models based on team feedback.
6. Week 6: Complete preliminary results for all approaches.
7. Week 7: Discuss results with team members and choose one approach to focus on. Investigate ways to strengthen and improve the chosen approach.
8. Week 8: Begin preparation of formal report and presentation of investigations. Start writing proposal for further research.
9. Week 9: Continue refining model in terms of data and algorithms and any refinements. Explore any variations or other ideas generated by research.
10. Week 10: Final editing of documentation. Presentation of results to management. Select future directions and collaborations.