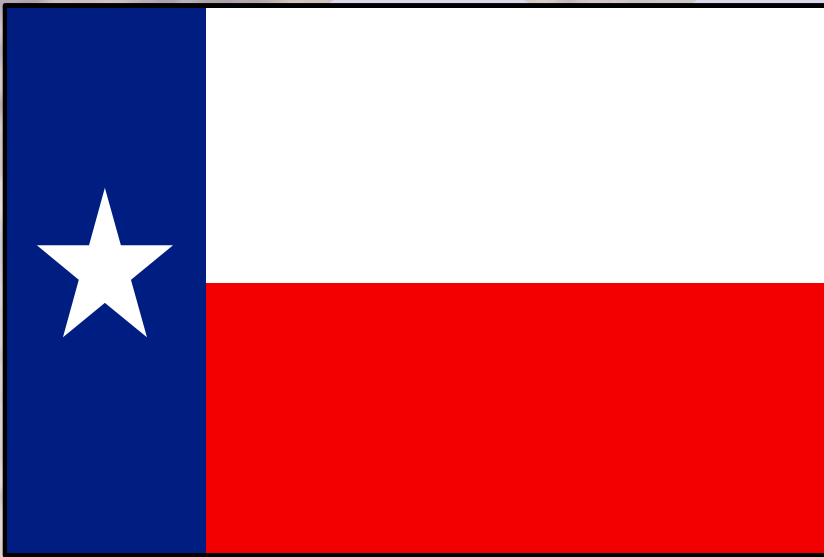


# 4<sup>th</sup> Information Survivability Workshop: Impediments to Achieving Survivable Systems



Larry Leibrock, Ph.D.

The University of Texas

© Larry Leibrock

3.13.02



# Today's Talk.

---

- I serve as the Chief Technology Officer for the Business School at the University of Texas.
- I am a professor at the University of Texas.
  - I teach Information Technology (Database Systems Analysis, Computer Security - Forensics Computing).
  - I also teach at the UT Law School - (Digital Evidence, Forensics and Systems Security).
  - I serve on the Texas - State Infrastructures Protection Committee (SIPAC)
- I have a range of incident response - digital forensic investigative experience and *at trial* - expert testimony.
- I am not a practicing attorney - you bear all risks of use of this material.
- Opinions, ideas and concepts do not represent official positions of any institution.



# My goals for today's talk - Teaching Systems Survivability

---

1. Describe the present set of barriers in achieving survivable systems in our time.
2. Speak to some present operational challenges in implementing and operating survivable systems
3. Conceptualize and Differentiate “*Theory and Practice*” teaching clinical approaches to the primary survivable systems
4. Frame some approaches to better research and teaching engagement
5. Stimulate your interests and ideas about this matter



# Survivability- Clinical Definition

---

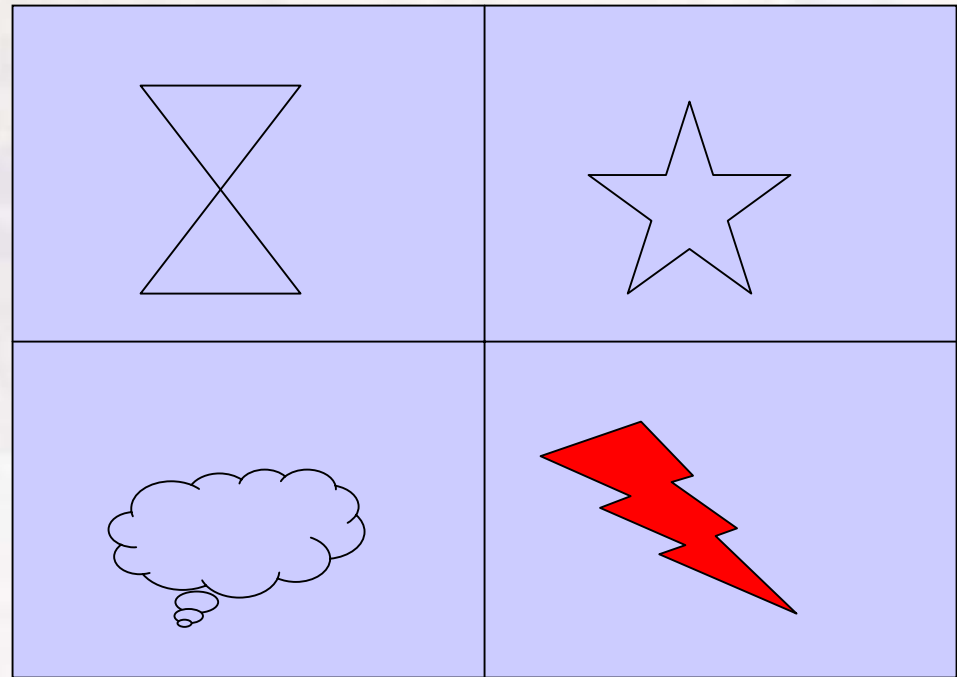
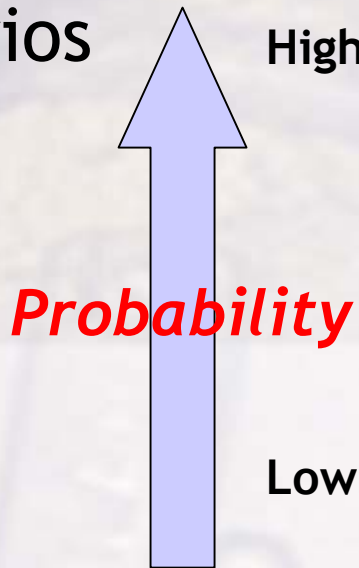
- As related to enterprise information systems (EIS) - systems survivability is the exploration, analysis, practices and stewardship of insuring that our enterprise informational environment can resist the range of expected attacks and continue to provide utility to its users.
- Survivable systems depend on automated, semi-automated or non-automated artifacts: (1) people (2) processes, (3) tools and (4) measures to maintain the band of service - specified in the enterprise service-level-agreement (ESLA).

*Larry Leibrock, 2000*



# Systems Survivability - post 9.11.01

- Low Probability/  
High Impact  
Scenarios



Low

High



# Survivable Systems - Value Proposition

---

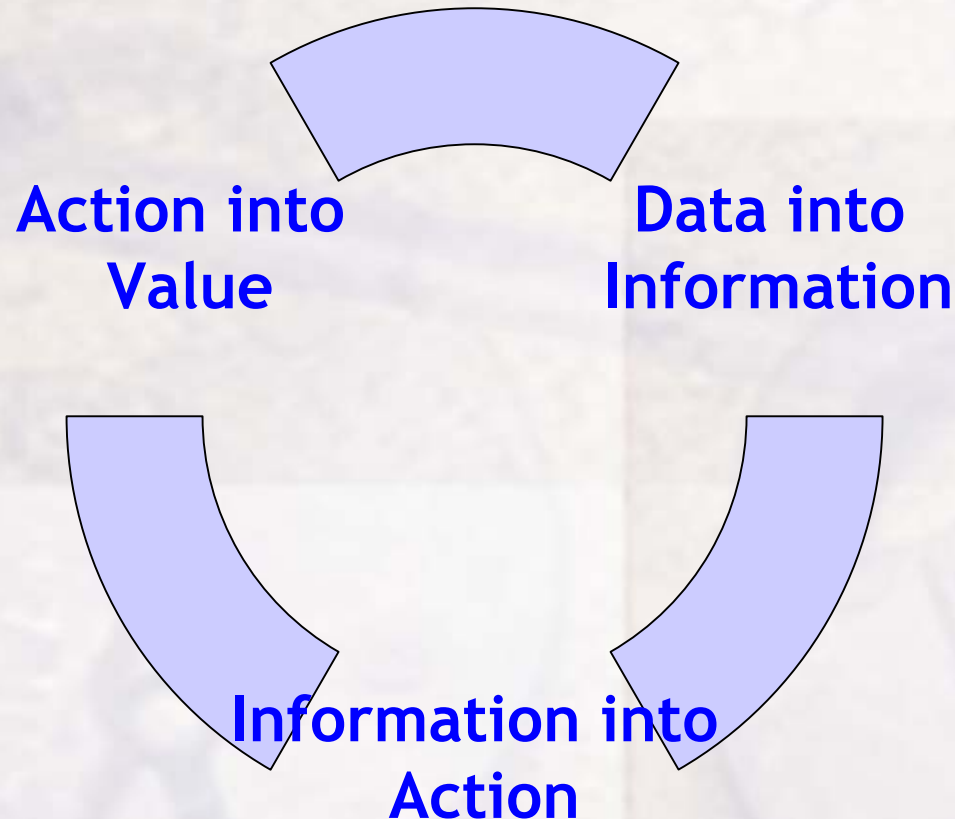
The sponsoring enterprise entity wants to achieve value in supporting systems survivable projects by:

1. Creating an explicit band-of-service based on an agreed service-level-agreement
2. Finding patterns based on risk data (transforming into useful enterprise threat and probability information)
3. Allocating necessary resources to mitigate risk
4. Detecting and triaging the range and severity of attacks
5. Acting (Responding) -- in a *timely* manner
6. Exercising stewardship to enterprise systems, reputation and data



# Survivable Systems - Value Proposition

---



# Challenges

---

- *The complexity of systems survivability practices has always dwarfed the simplicity of computer security/survivability theory.*
- The “vocabulary” of security experts have served to disengage organizational “resource-providers”
- These “resource-providers” will not invest in what they do not understand.



# Survivable Systems- The Inherent Task Areas

---

1. Explicit Classification of Band of Service
2. Estimation and Prediction of Risk-Threat
3. Mitigation plan and time-based assessment
4. Implementation and Deployment
5. Operations
6. Detection - Response
7. Recovery - Forensics



# Survivable Systems - Converging Drivers

---

1. Increased global competition for buyers/suppliers/services/information providers. (*enterprise data stores are the heart of modern business and government processes.*)
2. Pervasive data production among business supply chains, value nets, e-Business, e-Government initiatives
3. Creation of distributed data warehouses



# Survivable Systems - Converging Drivers

---

4. Increased low-cost computational power among networks - both client/server and peer-2-peer architectures
5. The rise of digital devices (PDA - Cell)
6. Development of better and more robust software toolsets
7. Better technical skills and increased professionalism in IS field.
8. Richer data types



# The “In-Practice” Survivable Systems Descriptive - Methodology

---

1. Identifying the problem (formal or informal framework or hypothesis testing).
2. Organizing and cleaning the data-sets
3. Select task areas -- focus on particular tool capabilities
4. Adjust derived models (iteratively)
5. Presenting results
6. Making judgments - Taking actions
7. Measuring outcomes -- prepare to adjust models, survivability operations and “systems robustness” over time



# The eTrading Server AKA iPremier Case A-B-C

---

- Setting
  - IT
  - Corporate Culture
  - Decisions
  - Shipping Product “urgency”
- Incident - DDOS
- Recovery
- Sanctions
- Demo “Stachel Dracht” DDOS



# MBA - Pedagogy - The - eTrading Server AKA now iPremier Case

---

## People + Processes + Tools + Measures

- (People) -- Exploration of “Failure *Chain*” in terms of probable systems, managerial and logistical needs
- (Processes) - Systems Survivability - How are business values and decisional options ranked
- (Tools) -- What are the ranges and derivation of planning, logistics, attack and post attack methods?
- (Measures) - Can technical and management better engage and collaboratively enumerate “*success and failure*” metrics?



# Present-day survivability operational challenges

---

- Availability of trained personnel -operations
- Data -- time, availability of resources, data quality, conversion of data-forms
- Data sizes - sampling - of logs
- Security- Assessment - Incident Response Methodologies and IT Project practice
- Asking the right questions --experimentation, proof of concepts, production, timeliness



# Systems Survivability - applications for practice and applied research

---

## One to Five year View -- Potential areas

1. Client/server and Peer to Peer (grid) computation models
2. Covert channels - Cryptography and Steganography artifacts.
3. Forensic tokens - disk - systems - applications - media/actor
4. Digital device "tool marks"--Digital cameras/photos - Palm Pilots/Windows CE - Phones - GPS - digital media
5. National Communications Infrastructure data sources - logs - registers - CVE Data Stores



# Systems Survivability -(continued)

---

## Two to Five year View -- Potential areas

6. Data-mining and systems security software agents -
7. Control Large Data sets (disks, networks and files)
8. Very fast symmetrical multi-processor systems (64-bit - Very Long Instruction word data-base servers)
9. Better body-of-knowledge in digital forensics - the emerging state of the **systems survivability guild**.
10. Better case teaching using integration of theory and practice
11. The survivable system as patient/doctor model



# Wrap-Up

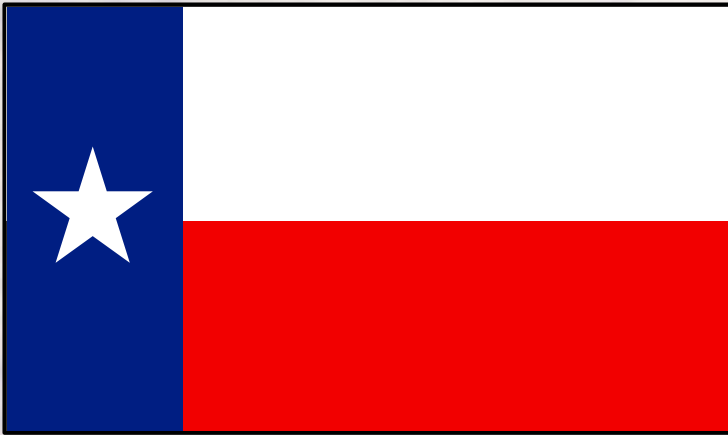
---

- Implications
  - Survivability Field: Better Theory - Practice Integration
  - Medical Models as a helpful Analog
  - Clinical Teaching - Focus on Case Model
    - Describe
    - Demonstrate
    - Let the Student Teach
- Your Reactions?
- Any Critique?



Thank you for your Attention to this talk

---



- I hope you have found this talk of value in meeting your professional needs.
- [Larry.L Leibrock@bus.utexas.edu](mailto:Larry.L Leibrock@bus.utexas.edu)
- [www.eForensics.com](http://www.eForensics.com)



