

University Teaching Models as an Impediment and Enabler to Teaching Systems Survivability: A Case Method - Field Experiment

Larry R. Leibrock Ph.D.,
The University of Texas -Austin, Texas 78755, USA,
Larry.Leibrock@eforensics.com

Key Terms

IS security, systems survivability, critical infrastructure, enterprise systems, computer forensics, mission-critical environments, clinical case teaching.

Abstract

The business, operations and governance of mission critical information systems and infrastructures is of increasing interest in many governmental, professional and university settings. Many important computer science and information science research initiatives have focused in knowledge development relative to the aforementioned areas of mission critical environments, enterprise systems, computer security and survivable infrastructures. Unfortunately, much of this research lacks integration and application to support our MIS and business operations practices. To better align research and practice skills the case “*The iPremier Case: The DDOS Attack*” was developed. As a field experiment the case has been taught to seek better integration and to build synergies between research and practice in these areas and particularly deal with issues of systems survivability¹.

Focus

The apparent prevailing focus on abstract theory and some extant lecture-based teaching models can serve to be counter-productive in teaching some technical information systems (IS) topics. The more clinically engaged teaching approaches, namely case class engagement, in the disciplines of enterprise systems management, information systems security, systems survivability and our emerging interest in protection of critical information infrastructures are thought to act as a change-driver for our learning models. These models are certainly important to support the effective teaching goals of both university and professional school settings. A clinical case “*The iPremier Case: The DDOS Attack*” was developed among three educators and practitioners.² This

collaboration was intended to serve as an experimental field-test vehicle to stimulate case discussion, increase managerial and technical dialogue related to systems survivability³. This cross-discipline dialogue is conceived to have better utility in making both strategic and operational judgments which affect IS and operations matters at the level of the firm. We posit that the interplay of both technical and managerial judgments are to be elicited about the overall efficacy, security and survivability of a given enterprise system. This interplay need is central to our development of the “*iPremier Case: The DDOS Attack*”. The case discussion is supported by an “in-situ” demonstration of a distributed denial of service attack on a closed network host platform. Learners are asked to make a successive set of operational, ethical and critical incident judgments and decisions as to enterprise systems operations, a distributed denial of service attack, systems recovery, concealment of material facts, communications to stake-holders and the utility of computer systems forensics.

1 THE PROBLEMS OF TEACHING THESE MATERIALS

The management of enterprise systems, particularly those in e-business settings has become increasingly central to both the strategy and operational success the firm. For

³ An information system is survivable if it is able to continue to provide service when it is faced with some form of attack and resulting damage. For example, if a computer system loses commercial power it usually stops operating completely. In many circumstances this is unacceptable but full service is not required. All that is needed is the continued provision of the most important services. If the computer has a backup power source, then the loss of commercial power need not stop everything.

More formally, survivability requires the definition first and foremost of the set of faults to which the system might be subjected. For each different fault, the system's owners need to define what continued service is required if that fault occurs. In some cases, no service might be an appropriate response. In others, full service might be required irrespective of the occurrence of the fault. In most cases, the requirement will be something in between. A survivable system is one that meets its requirements for each type of fault (CERT).

¹ Survivability of a system can be expressed as a combination of *reliability*, *availability*, *security*, and human *safety*.

² The iPremier Case, Harvard Business School

the non-technical learner, these are sometimes seen as quite complex and abstract. In some business settings enterprise systems management was traditionally seen as generally under the purview of technical, administrative or financial control functions in organizational. The rise of global networks, interoperating supply chains, corporate data stores, e-business requirements and customer-facing technologies have seen more demands for mission-critical operations and more robust stewardship of these enterprise-wide information infrastructures. What previously was primarily seen as a technical concern is now increasingly viewed as both an overarching business strategy and general management operational problem. Business leaders and executives are expected to play an increase role in the collaborative responsibilities of managing the operations and overall protection of these information infrastructures. To better prepare these learners, researchers and academics should stimulate practical attentions to issues central to information systems management, security, survivability and critical information infrastructures. These are abstract concepts that typically are viewed as technical topics not deserving executive attentions. The premise of our approach was to depart for the lecture approach to a more applied case method supported by a concrete demonstration of a distributed denial of service attack against a server system as one exemplary attack against the survivability of a system⁴.

2 THE CASE APPROACH

To prepare for the case learning process, students were given a set of pre-class readings. The readings set out the “*The iPremier Case: The DDOS Attack*” “A” case, a separate reading about computer intrusion, hacking attacks, and a set of case related questions. Students were asked to use WWW to stimulate inquiry and prepare responses to questions about these topics:

1. As a business executive, do you have enough information to make an operational – systems survivability decision in this case setting?

⁴ An extreme range of causes or sources can lead to failure although there is considerable concern about security attacks. Most major failures have been from other sources. A non-exhaustive list of the most important sources of failure and survivability includes:

1. Human errors
2. Errors in operational procedures
3. Changes in environmental conditions (power)
4. Software faults
5. Software media failures
6. Software design degradations
7. Hardware degradation faults
8. Hardware design faults
9. Malicious attacks

2. What are some categories of attacks (malicious – non-malicious) and risks (low probability – high probability) to an enterprise system in the “A” case?
3. What are some non-technical and technical notions of systems survivability material to the “A” case?
4. Does the concept of systems survivability only concern malicious acts or can it deal with such problems as poorly designed software or defects in particular hardware components and systems?
5. Can you enumerate a range of objects that should be protected in systems survivable settings.
6. Relative to an enterprise system, what is a risk assessment, what are some strengths and weaknesses of these risk assessments?
7. Does a hacking attack (intrusion) or a distributed denial of service against an enterprise system constitute a crisis for the firm?
8. How can the executive best make judgments and decisions under a crisis situation?
9. Given some indications (facts, knowledge, data and observations) of an apparently successful systems intrusion what actions should the executive consider?
10. Given our notions of both ethical and legal responsibilities, what should be some primary concerns of the executive related to:
 - Duties to stakeholders of the firm
 - Customer trust,
 - Privacy of data,
 - Duty to report to law-enforcement
 - Down-stream liability, systems survivability and
 - Business reputation?
11. In e-Business and enterprise settings, what are the roles of:

- corporate controls,
- audit processes,
- systems-incident response and
- computer forensics?

Case participants and engaged learners are advised to carefully think about, critically assess and prepare these responses to these above questions. Responses to the questions are to be in note form and students should be prepared to make a set of operational and business judgments as managerial “actors” in the “*The iPremier Case: The DDOS Attack*” The participants are also advised to consult WWW search engines in order to collect more complementary information to aid in making clear some working definitional constructs related to the case questions and the facilitator case plan. Some notions and constructs include: hackers, denial of service, first-response, systems survivability, computer incidents, crisis management and enterprise systems.

2.1 The General Case Progression

These pre-class instructions are validated by a set of cold-calls and student responses. Typical set student responses seek to delegate responsibility to some information technical executive. Secondly, some students seek to form an enterprise crisis response team to provide better data, fact-based observations, decisions and responsive actions to support this enterprise systems crisis. The case facilitator provides a set of more detailed “B” and “C” level cases which are intended to serve to inject more information, more knowledge, and more uncertainty in order to require more decisions from these learners. Subsequent to the “C” case a denial of service demonstrations is conducted against a closed network web server. The more technical details of the distributed – denial of service “Stachel Dracht” tool is described. Motivations and rationales for these malicious attacks are discussed after the demonstration. Systems intrusions versus packet-network attacks are described. In a grounded practice fashion supported with an after-action review of the case and consequences of managerial actions and inactions is presented. A set of Computer Emergency Response Team CERT® and Federal Bureau of Information - National Infrastructure Protection Center NPIC® advisories which pre-dated the particular attack are presented. To conclude the case learning experience a set enterprise systems survivability practices are presented for the students.

2.2 Case Reactions

Both for the involved faculty and learners, reactions have been very positive about this clinical case. The range of perspectives, questions and insights were beneficial. The in-class distributed denial of service (DDOS) demonstration was well received. The experimental use of this learning vehicle has resulted in wide-ranging interest,

after-class comments and thinking about managerial frameworks to support decisions and actions for enterprise systems management, security survivability in critical infrastructure settings. Anecdotally, we have been approached on preparing these cases to support learning in MIS deployments, security and privacy of data, global network operations, systems cryptography, steganography and forensics.

2.3 Global Settings.

As of March 2002 *The iPremier Case: The DDOS Attack* has been taught at five universities in the US, Mexico, Finland and Singapore. The purpose of this global focus has been to stimulate interest in our thinking about global connectivity, systems stewardship, inter-operating critical infrastructures and international systems survivability concerns.

3.0 EXPLICIT TEACHING “IN-PRACTICE” CASE METHODOLOGY

The following sequence is the explicit teaching model for this case.

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

3.1 Subjective Assessment

During the case progression students are asked to review figure 1 which is meant to stimulate insights into the efficacy of planning and responding to attacks in impact (strategic and operational) versus probability of occurrence.

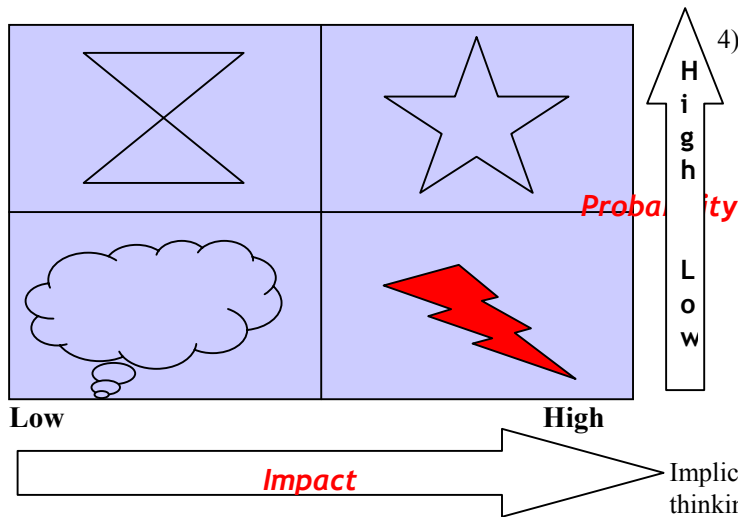


Figure 1: Model for Impact versus Probability Matrix

4) **Measures** – Can technical and management better engage and collaboratively enumerate “*success and failure*” metrics?

5.0 CONCLUSIONS

Implications are tentative in but interesting in our thinking about this experimental field study and case development. Enterprise systems management, protection of critical information infrastructures and systems survivability is increasingly important topics of interest in our recent times, especially given the unfortunate events of September 11, 2001. The theory and experimentation of the present level of IS and MIS research, IS security and systems survivability are useful and fruitful – however in themselves, they are insufficient in supporting the needs of professional teaching. We should consider the better these issues:

- 1) Better Theory – Practice Integration to support increased professionalism in enterprise systems management, systems survivability and critical informational infrastructures.
- 2) Consider the utility of medical models as a helpful clinical analog (observation, orientation, decisions and actions)
- 3) Develop more clinical teaching materials, based on field studies – Focus on case discussion & demonstration model
- 4) Develop more field cases that do the following:
 - Describe the problem
 - Demonstrate some cause/effect
 - Engage - Let the students teach the primary points with case facilitation

4.0 PEDAGOGY - THE IPREMIER CASE

The “*The iPremier Case: The DDOS Attack*” case makes use of a particular decisional framework People + Processes + Tools + Measures

- 1) **People** -- Exploration of “*Failure Chain*” in terms of probable managerial actors, communications and logistical needs.
- 2) **Processes** – Systems Survivability - How are business, operations, values and decisional options ranked?
- 3) **Tools** -- What are the ranges and derivation of planning, logistics, pre-attack and post attack tools?

5 ACKNOWLEDGEMENTS

I wish to thank CERT®, the Information Survivability Workshop and my colleague Dr. Rob Austin at the Harvard Business School for supporting this work and serving the community of practice in the emerging field of systems survivability.

