IDEA GROUP PUBLISHING
701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

ITB12711

This paper appears in the book, *Emerging Trends and Challenges in Information Technology Management, Volume 1 and Volume 2* edited by Mehdi Khosrow-Pour © 2006, Idea Group Inc.

Target, Shield and Weapon: A Taxonomy of IT Security Initiatives

Laura Lally, Hofstra University, BCIS/QM Department, Hempstead, NY 11549-134
{Phone: 516 463-5351, E-mail: acslhl@hofstra.edu}

ABSTRACT

With IT Security becoming an issue of growing importance, many new IT based technologies and applications are emerging to confront this challenge. This paper presents a theoretically based model for classifying these emerging technologies, the "Target, Shield and Weapon" model. The goal of this research is to create a meaningful taxonomy for emerging initiatives that will: 1) ensure interoperability with existing, and other emerging systems, 2) identify areas of basic research needed to support the full operability of these initiatives and 3) identify applications, developed for military scenarios that can be modified for use in civilian environment .Two case studies will be outlined for the application of the model: 1) the London terrorist bombings, and 2) the New Orleans flood.

A THEORY BASED MODEL FOR CLASSIFYING NEW INITIATIVES IN IT SECURITY

IT Security has become an issue of great importance. The increase in malicious computer based attacks, the Y2K crisis, the events of 9/11, and the growing dependence on networked computer systems have made the security of IT based systems a top priority.

Even though computer budgets are being cut, spending of security has increased. An increasing number of entrepreneurs are developing solutions for these problems. New government regulations require that organizations keep their systems more secure and keep better track of their documents. MIT's Magazine of Innovation: Technology Review reports that the budget for the 2005 Department of Homeland Security for 2005 was $30 billion dollars (MIT's Magazine of Innovation, 2005). For Customs, Immigration, and Border Protection it included $2.9 billion for container security and $340 for US-VISIT, an automated entry and exit system for frequent international travelers For the Coast Guard, it included $724 million to upgrade the technology and communications division. For the Transportation Security Administration $475 million for explosives detection systems, baggage screening equipment and their installation. For State and Local Assistance programs it included $150 in port security grants, $150 million in rail/transit security grants and $715 million in grants to fire departments. For the Emergency Preparedness and Response Directorate, it included $2 billion for an emergency relief fund. For the Science and Technology Directorate, it included $593 million to develop technologies that counter threats from chemical, biological, nuclear and radiological weapons and high explosives and $61 million to continue the development of innovative countermeasures to protect commercial aircraft against possible missile systems. For Information Analysis and Infrastucture Protection Directorate, it included $2 billion to assess and protect critical infrastructures including cyberspace. "Pasadena, CA-based Cogent, which developed automated fingerprint recognition systems used by law enforcement and the Department of Homeland Security, went public in September and raised $216 million, then saw its stock price nearly triple by the end of the year (MIT Magazine of Innovation, p.42).

As a result of this new emphasis, many new IT based initiatives have evolved. This paper proposed a theoretically based model for understanding three functions security based initiatives can serve. First, since IT based systems are often a target of malicious attacks, security initiatives can intercept intrusions before they can do damage. If attacks do occur, other IT based systems can mitigate the damage that is done, both to computer systems and to the real world systems that depend on them. Secondly, IT based initiatives can suggest best organizational practices to shield against further attacks. Finally, IT based initiatives can be used to proactively seek out potential attackers and prevent them from launching first attacks.

This taxonomy will be used to categorize the functionality of initiatives as they emerge and address several key challenges and opportunities faced by the developers of new security initiatives. First, the challenge of making new initiatives *interoperable* with existing systems will become more apparent. Secondly, with venture capitalists putting an increased emphasis on the development of systems that can be made operational within a short time frame, the need for *basic research* that must be explored to make the initiatives fully operable will be more easily identified. This basic research can then be fast tracked and its cost allocated between all the applications that depend on it. Finally, opportunities for *additional applications of emerging technology*, such as military applications being used to help first responders will be more apparent as well.

This paper will draw on Lally's "Target and Shield" model (Lally, 2005) a theoretically based model for examining the potential threats to IT based systems, the propagation of these threats, and the potential for their mitigation. The paper will then extend the model to encompass the use of IT as a weapon against potential attackers.

Finally, a taxonomy of emerging initiatives will be created to illustrate the appropriateness of the model in categorizing these initiatives.

Lally's "Target and Shield" model is based on Normal Accident Theory, originally conceived by Charles Perrow (Perrow, 1984) as a model for how small errors can propagate into large disasters. The model is also informed by the Theory of High Reliability Organizations, that emphasizes methodologies by which organizations can minimize the likelihood for disaster in tightly coupled complex organizations (Grabowski and Roberts, 1997), (Klein, Bigley, and Roberts, 1995), (LaPorte and Consolini, 1991), (Sagan, 1993), (Turner, 1976), and (Weick, 1993).

Lally (1996) argued that Normal Accident Theory was a sound theoretical perspective for understanding the risks of Information Technology, because IT is complex, and tightly coupled and often poorly controlled. She also argued (Lally, 1996), (Lally, 1997) that IT based systems do not operate in isolation but in organizational settings where failures in IT can lead to more widespread secondary failures in organizations. Additionally, she argued (Lally, 2002) that the frequent rapid change in both IT based systems and the work processes they support can further exacerbate the potential for disaster. Lally (2005) further extended her model and argued that IT based systems are not only a target used as a weapon of destruction to cause serious accidents, but that IT based systems can be a shield used to prevent damage from future incidents, whether they be IT based or physical. This "Target and Shield" conceptual model drew on insights from the Theory of High Reliability Organizations and suggests that IT designers and managers, as well as

Figure 1. The target and shield model

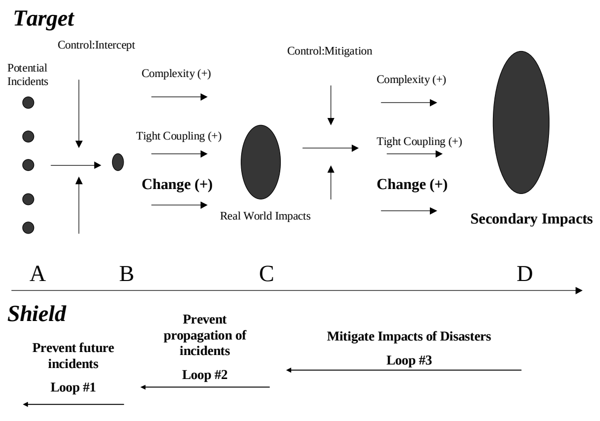
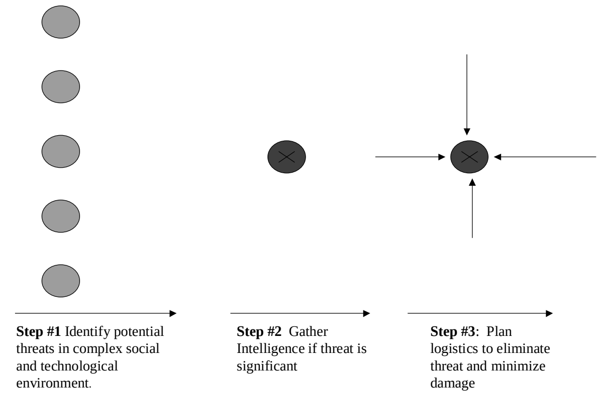


Figure 2. IT as a weapon against potential threats


Step #1 Identify potential threats in complex social and technological environment.
Step #2 Gather Intelligence if threat is significant
Step #3: Plan logistics to eliminate threat and minimize damage

government and law enforcement agencies learn from past experiences and embody this knowledge in the design and implementation of future IT based systems. The resulting systems should not only be more secure and resilient, they should aid in preventing future IT based or physical attacks, or mitigating their impact should they occur. Figure 1 illustrates the Target and Shield conceptual model for analyzing the source, propagation and impacts of IT based threats, as well as ways in which IT can be used to identify, and mitigate the impact of, future threats.

The Target and Shield model incorporates Lally's extensions to Normal Accident Theory. The model also contains *three significant feedback loops*, which allow IT to play a positive role in preventing future incidents from materializing, having real world impacts, and mitigating their impacts when they do occur. In the Feedback Loop #1, Prevent future incidents, controls can be built into the system to prevent future incidents from materializing.

In Feedback Loop #2, Prevent Propagation of Incidents, controls can be built into the system to prevent future incidents that have materialized from turning into accidents.

In the Feedback Loop #3, Mitigate Impact of Disasters, IT based systems can be dev eloped to prevent accidents resulting from IT based or physical attacks from propagating even further.

Lally and Nolan (2005) applied the Target and Shield model to map Wireless Technologies. Their analysis indicated that Wireless Technologies are a Target because of their vulnerabilities to Air Interface denial of service attacks, snooping attacks that threaten data integrity and the limitations of standards in applications that use unlicensed spectrum. Their analysis also indicated that Wireless Technology could be used as a shield because the distributed architecture of these networks can provide robustness and redundancy to prevent catastrophic failures. Finally, they indicated that location aware devices could be used for tracking suspected cyber attackers.

EXTENDING THE MODEL: IT AS A WEAPON

In the Target and Shield Model, Feedback Loop #1 addresses the challenge of preventing future incidents. In a learning environment, once incidents occur, knowledge should be gained about the nature of the incident to prevent future incidents from occurring. The proactive prevention of future incidents involves more than waiting for new incidents to occur and developing defensive techniques when they do. IT Based tools are emerging for tracing incidents to their source and eliminating them. When IT is used as a weapon to fight back against potential attackers, the dynamics of the "Target and Shield" model is reversed. Instead of responding to a single negative event and its propagation through a large and complex system, the emphasis is on identifying potential threats in a complex technological and social environment, gathering intelligence on those threats, and if the threats are confirmed, planning the logistics to eliminate the threat with a minimum of damage to innocent people and their property. With use, the model should also provide insight into which threats are the most serious and need to be eliminated.

In Step #1, IT can be used to identify anomalous behavior, such as a group of people who have never contacted one another suddenly being in frequent contact. Artificial Intelligence based systems for identifying anomalous patterns in telecommunication behavior can identify unusual patterns. The challenge in Step #1 is identifying potential threats in an environment that consists primarily of innocent people, whether corporate employees or civilians. In Step #2, IT based intelligence gathering can then reveal whether the members of the new group are on a "watch list"—indicating that they may be a terrorist cell becoming active, or, perhaps members of a new computer class, corporate subcomittee or scout troop. In Step #3, if the threat is real, IT can then be used to monitor the activities of the group and eliminate the threat in a manner that will cause the least collateral damage.

Many new IT based tools are being developed for military applications that can be mapped into the model. These applications can be modified for use in non-combat situations. In "Network Centric Warfare" the U.S. military uses Information Technology as a force multiplier with the hope that it will lead to shorter conflicts with limited casualties to armed forces and civilians. The three crucial elements of the strategy are to provide troops with additional strategic advantages in terms of: 1) knowledge of both enemy and allied troop movements, 2) speed to respond rapidly, and 3) precision, leading to more surgical strikes.

Applications include highly detailed surveillance and GPS data to provide soldiers in the field with up to date information about local terrain and the presence of enemy tanks. Frontline soldiers in sophisticated Stryker vehicles and command centers are kept in constant contact. Military strikes can be more surgical so that innocent civilians and their property, as well a cultural landmarks can be protected. Step #3, therefore, appears to be well suited for enhancement with IT support. The emphasis by the military on using Commerical-Off-The-Shelf technologies makes the possibility of trickle down effects for civilian applications more likely. The emphasis by the military on convergence at the client server or at the TCP/IP level, where information is shared via the Internet, even to users who may use different technologies to access the information. Similar technologies can be used to help first responders create more co-ordinated responses to threats. The interoperability of the technology, and its reliability, are of primary importance. GPS enabled systems used by the military can also be used by first responders as well as by businesses to provide a wide range of location based services.

Although surveillance technology can identify enemy tanks, Step #1, identifying potential threats in civilian populations provides a far greater challenge. Simulation games are being developed (NPR, 2005) to help soldiers to interact with civilian populations who have different languages and culture to facilitate the process of interaction and minimize the potential for misunderstandings. First responders in multicultural urban areas could also use these games to familiarize themselves with the cultures, languages, and social conventions of different ethnic groups that could help construct a more appropriate means of interacting with the public. Step #2, the identification of actual, versus potential threats can also be supported with database technology, if correct information is gathered and shared about potential threats. The minimization of false positives here is key for the civilian population to retain confidence in the system.

The degree to which technology can support these two stages, obviously varies widely. As other initiatives emerge and are analyzed, the model should indicate to military commanders, chiefs of first responder units and organizational leaders, the degree to which technology can support a given phase of threat elimination.

TWO MAJOR DISASTERS: THE LONDON TERRORIST BOMBINGS AND THE NEW ORLEANS FLOOD

Two major disasters occurred in the summer of 2005. The London terrorist bombing and the New Orleans flood. Case studies of both disasters will be developed in terms of the Target, Shield, and Weapon (TSW) model.

The London terrorist bombing, like 9/11, was the result of a terrorist plot. The TSW model will provide insight into:

- What existing Information Technologies exist that could have prevented the bombings? Could the use of databases and surveillance technologies (widely used in London) uncovered the plot before it occurred? What emerging technologies can enhance the likelihood that future attacks can be prevented?
- How was Information Technology used to mitigate the damage of the attack? How was communication technology used to coordinate rescue efforts? What existing and emerging technologies can further improve rescue efforts after a terrorist attack?
- How was Information Technology used to track down the bombers? How did London's elaborate surveillance system trace the bombers back to their supporting organizations? What existing and emerging technologies can enhance the ability to track down and eliminate future threats?

The New Orleans flood was a disaster of natural origins. The TSW model, however, can still provide insights.

- What Information Technologies could have predicted the problem and designed solutions? Preliminary evidence suggests that simulation models had already predicted the vulnerability of New Orleans' levees to Class 4 hurricanes and that designs for solutions were in the blueprint stage. How can existing and emerging technologies identify future disasters from occurring? Furthermore, how can information resulting from these analyses be conveyed and acted upon before predicted disasters occur?
- Given the advances in first responder technologies and methodologies since 9/11, what went wrong in New Orleans? What existing and emerging technologies can enhance the ability of first responders to conduct well co-ordinated and effective rescue and evacuation efforts?
- Since a hurricane is a natural disaster, it is unlikely that IT can prevent future storms from materializing.

In both cases the taxonomy provided by the TSW model will provide insights into which Information Technologies are already available, which are emerging, and what further basic research needs to be done. Insights into which Information Technologies developed to counter terrorism can be applied to predict and to mitigate the impact of natural disasters should also emerge.

REFERENCES

Grabowski, M. and Roberts, K. (1997). Risk mitigation in large scale systems: Lessons from high reliability organizations. *California Management Review*, Summer, 152-162.

Klein, R.L., Bigley, G.A., Roberts, K.H. (1995). Organizational culture in High Reliability Organizations. *Human Relations*, 48:7. 771-792.

Lally, L. (1996). Enumerating the risks of reengineered processes. *Proceedings of 1996 ACM Computer Science Conference*, 18-23.

Lally, L. (1997). Are reengineered organizations disaster prone?" *Proceedings of the National Decision Sciences Conference*, 178-182.

Lally, L. (2002). Complexity, coupling, control and change: An IT based extension to Normal Accident Theory. *Proceedings of the International Information Resources Management Conference*, 1089-1095.

Lally, L. (2005) Information Technology as a Target and Shield in the Post 9/11 Environment. *Information Resources Management Journal*, Jan-Mar, Volume 18, No. 1.

Lally, L. (2005). Applying the Target and Shield Model to Wireless Technology, *Proceedings of the International Information Resources Conference*, upcoming.

LaPorte, T. R. & Consolini. P. (1991). Working in practice but not in theory: Theoretical challenges of High Reliability Organizations. *Journal of Public Administration,* 1, 19-47.

Perrow, Charles. (1984). *Normal Accidents: Living with High Risk Technologies.* New York: Basic Books.

Sagan, Scott. (1993). *The Limits of Safety*. Princeton New Jersey: Princeton University Press.

Turner, B.M. (1976). The organizational and interorganizational development of disasters. *Administrative Science Quarterly*, 21, 378-397.

Weick, K.E.and Roberts, K. (1993). Collective mind in organizations: Heedful interrelating on flight decks. *Administrative Science Quarterly*, 38, 357-381.

ENDNOTE

* This research was funded by a Summer Research Grant from the Frank G. Zarb School of Business at Hofstra University.