Employing Dynamic Models to Enhance Corporate IT Security Policy

Nathan A. Minami, Virginia International University, USA

ABSTRACT

Since 9/11 and the creation of the U.S. Patriot Act, the intrusion of government surveillance into the lives of ordinary Americans has become a topic of great concern to many citizens. While many Americans view surveillance as a necessity in the name of national security, the government is not the only organization conducting surveillance. As technological capacity increases, an increasing number of employers are implementing technologies that allow them to maintain vigilance over the actions of their employees in the workplace. Despite many attempts to implement surveillance technologies, there is little evidence that companies are any safer now than they were ten years ago. This paper demonstrates how System Dynamics modeling can be utilized to help model the insider threat as a system. It provides analysis of the non-linear affect of decision making, assessing the 2nd, 3rd, and 4th order impacts of decisions, and demonstrates the important impact of delays in the system. A mathematical model is presented and simulations are conducted to determine the likely affect of company decisions and individual agent behavior.

Keywords: Dynamic Modeling, Employee Monitoring, Information Technology, Simulation, System Dynamics

INTRODUCTION

The events of 9/11 and subsequent governmental actions such as the Patriot Act brought the topic of personal privacy to the fore as most Americans expect to have a degree of privacy when not in a public forum. In addition to national security concerns, globalization and advent of the internet and numerous other technological innovations have made employee monitoring in the workplace a perceived necessity for many companies (Latto, 2007). The fact that 82% of employers conduct electronic monitoring in some form has made the topic one of great debate for many Americans and their employers (Tabak & Smith, 2005). Indeed, companies have the right to protect their intellectual and physical property, but it is not clear whether it is more important to protect personal privacy or company property. This paper provides an extensive literature review of the problem and then demonstrates how systems analysis and mathematical modeling using the System Dynamics modeling procedure can help to better explain agent behavior within the individual company.
LITERATURE REVIEW

The following review of the literature is critical to this study because it describes the increasing problem of insider attacks. It also provides the background and logic for the mathematical model that is built and presented later in the paper.

Privacy and 9/11

Since the beginning of the War on Terror and implementation of the Patriot Act, few topics have been the subject of as heated debate as the conflict between security and civil liberties. One of the central topics of this debate has been the use of surveillance within the United States as a means of collecting intelligence. Surveillance is critical to homeland security as it is one of the best means of collecting actionable intelligence against terrorist organizations. But there is substantial conflict between civil liberties that are fundamental to America’s national fabric and surveillance that is necessary to ensure domestic security (Taipale, 2006). Consequently, a great deal of debate has occurred the last few years regarding the Patriot Act, with wire tapping and other forms of surveillance leading the discussion.

Historically during time of war the nation has typically tightened the noose on civil liberties and then loosened it some during times of peace (Rosenzweig, 2006). 9/11 may have changed the public’s tolerance, however, for the amount of risk they are willing to take in exchange for protecting basic civil liberties (Rosenzweig, 2006). Traditionally America’s legal system has been based on the idea that it is better to let the guilty go free than to punish the innocent. But in the age of global terrorism where the guilty might be a terrorist bent on destruction of the country, this premise may be challenged. On the other hand, if America is not careful, the terrorists may win the war simply by turning its enemy into a police state.

Another dominant issue following 9/11 is that U.S. federal agencies began ease dropping on virtually every mosque in the country, particularly targeting those that took a very fundamentalist stance in their approach to religion (Foxman, 2006). Some have argued that by racially and religiously profiling, the people of these groups become alienated against the government which can have drastic consequences. Indeed, this could cause law enforcement officials to miss terrorists in the event that a terrorist does not meet a racial profile (i.e., Timothy McVeigh). Still, there is another case to be made that profiling, in and of itself, does not work (Murphy, 2006). A parallel issue is control of radical clerics in the U.S. who openly speak out in support of terrorist actions against the U.S. government. While it may seem obvious that these clerics should be arrested or at least monitored, the utility of targeting these individuals is questionable. The reason for this is that aggressive action may only cause them to go underground and will likely have the unintended side effect of alienating much of the Muslim population.

There is little doubt that in order to protect the country from terrorists, Americans will have to make some concessions regarding their civil liberties (Taipale, 2006). One specific area where the debate of civil liberties versus security has come to the fore exists in the workplace. Specifically, there is much dispute about whether it is more important to protect a company’s intellectual property (IP) or guarantee the privacy of employees when using the internet at work. The following discussion examines this issue in depth.

The Insider Threat to Public and Private Companies

Insiders with malicious intentions pose a tremendous threat to companies; this is especially the case in the banking and finance sectors (Ran-dazzo, Keeney, Kowalski, Cappelli, & Morre, 2005). While insider attacks against companies have certainly been around for centuries, the phenomenon gained attention in the 1980s as companies became more reliant on computers and other information technologies that many employees could access (Chinchani et al., 2005).
On Drives
www.igi-global.com/chapter/drives/5091?camid=4v1a