Chapter 7
Social/Ethical Issues in Predictive Insider Threat Monitoring

Frank L. Greitzer
Pacific Northwest National Laboratory, USA

Deborah A. Frincke
Pacific Northwest National Laboratory, USA

Mariah Zabriskie[1]
Pacific Northwest National Laboratory, USA

ABSTRACT

Combining traditionally monitored cybersecurity data with other kinds of organizational data is one option for inferring the motivations of individuals, which may in turn allow early prediction and mitigation of insider threats. While unproven, some researchers believe that this combination of data may yield better results than either cybersecurity or organizational data would in isolation. However, this nontraditional approach yields inevitable conflicts between security interests of the organization and privacy interests of individuals. There are many facets to debate. Should warning signs of a potential malicious insider be addressed before a malicious event has occurred to prevent harm to the organization and discourage the insider from violating the organization's rules? Would intervention violate employee trust or legal guidelines? What about the possibilities of misuse? Predictive approaches cannot be validated a priori; false accusations may harm the career of the accused; and collection/monitoring of certain types of data may adversely affect employee morale. In this chapter, we explore some of the social and ethical issues stemming from predictive insider threat monitoring and discuss ways that a predictive modeling approach brings to the forefront social and ethical issues that should be considered and resolved by stakeholders and communities of interest.

DOI: 10.4018/978-1-61692-245-0.ch007

INTRODUCTION

In this chapter, we explore some of the social/ethical and privacy issues that may arise from attempts to protect information assets from crimes (including but not limited to espionage and sabotage) perpetrated by employees and trusted "insiders." Espionage and sabotage involving computer networks are among the most pressing cybersecurity challenges that threaten government and private sector information infrastructures. Surveys, such as the 2004 e-Crime Watch Survey (CERT 2004), reveal that current employees are thought to pose the second-greatest cybersecurity threat (22%), exceeded only by hackers (40%). Categories such as former employees (6%), current/former service providers (4%), foreign entities, competitors, and the like are perceived as much less likely sources. The insider threat is manifested when individuals do not comply with established policies, whether the noncompliance results from malice (malicious insiders) or a disregard for security policies. The types of crimes and abuse associated with insider threats are significant; the most serious include espionage, sabotage, terrorism, embezzlement, extortion, bribery, and corruption. Malicious activities include an even broader range of exploits, such as copyright violations, negligent use of classified data, fraud, unauthorized access to sensitive information, and illicit communications with unauthorized recipients. The insider threat also includes unintentional actions by individuals who inadvertently or unknowingly provide access to outsiders, such as in phishing and other attacks. For the purposes of the present discussion, we shall limit our scope to crimes or attempted exploits by malicious insiders.

The "insider" is an individual presently or previously authorized to access an organization's information system, data, or network. In many organizations, these individuals knowingly accept a commensurate level of scrutiny from their organization, meant to deter or detect abuse of these privileges. Insiders represent an especially insidious threat to organizations if they are careless or malicious. As trusted employees, they are permitted by the organization to have access to information and systems that could compromise the organization if misused. In deliberately proffering trust, the organization also decides in advance whether the risk outweighs the advantages, and presumably could withdraw such trust if it so chooses.

"Insider threat" for our purposes refers to harmful acts that trusted insiders *might* carry out—for example, something that causes harm to the organization or an unauthorized act that benefits the individual. A U.S. Department of Defense (DoD) Inspector General report (1997) found that 87% of identified intruders into DoD information systems were either employees or others internal to the organization. More generally, recent studies of computer crime or "cybercrime" –such as the CERT *E-Crime Watch Surveys* (CERT, 2004, 2005, 2006, and 2007; see also Keeney et al., 2005) in both government and commercial sectors– reveal that the proportion of (reported) insider threat exploits has ranged from 31% in 2004 to 49% in 2007, and the financial impact and operating losses due to insider intrusions are increasing. Insider crimes are not only a financial concern for employers; they also yield societal costs in the form of short- to long-term physical and emotional pain, lost opportunities, and additional "protection" mechanisms that society puts in place to prevent, detect, and respond to such threats. These costs are borne by individuals and organizations. To the extent that predictive insider threat monitoring can reduce risks and costs to organizations and society, the greater the benefit to society in terms of capacity to invest in other priorities. This too, is part of the promise of predictive insider threat monitoring. We hope that this chapter will provide input for those seeking to begin, or continue, this conversation.