How can we Model the Enemy of IT

Stewart Kowalski and Jeffy Mwakalinga

SecLab,

Department of Computer and Systems Sciences,

Stockholm University/Royal Institute of Technology,

Stockholm, Sweden.

ABSTRACT

Information systems are more and more being designed with the end user and usability in focus. However one important area that is current not being modelled or designed for is what can be referred to as end abusers. The enemy of IT seems to be always left out of a systems design. Sun Tzu said, 500 Before Christ, that if you know your enemy you have better chances of winning the battle. This paper describes a way of modelling the enemy of IT. The enemy uses different methods depending on the environment of IT. The enemy in friendly environments differs from the enemy in hostile environments. This model of the end abuser is based on the socio-technical economic model.

The Social-technical-economical model addresses security problems at social, logical, and physical levels. The model is based on value based chains. The value chain model for information security consists of functionalities: deterrence, prevention, detection, response, and recovery measures. The enemy uses the social layer for social engineering and creates attacks like phishing. The attacker applies the second layer, the logical layer, to automate some of the attacks by using for example software agents. After the enemy collects the information using the social layer could use software agents to extract the targeted secrets. The enemy uses the physical layer, to attack physical protection systems. This model will help researchers to develop better security systems.