SIXTH ANNUAL SYSTEM DYNAMICS CONFERENCE
JOINTLY HOSTED BY THE SOUTH AFRICAN SYSTEM DYNAMICS CHAPTER AND ESKOM SOC

Johannesburg, 22-23 November 2018

System Dynamics Modelling to Investigate the Cost-Benefit of Cyber Security Investment

Dr. Rudolph Oosthuizen *[1,2], Prof. Leon Pretorius [2], Francois Mouton [1], Mirriam Molekoa [1]

*[1] *Defence Peace Safety and Security, CSIR and Department of Engineering and Technology Management, University of Pretoria, roosthuizen@csir.co.za*

[2] *Department of Engineering and Technology Management, University of Pretoria, leon.pretorius@up.ac.za*

(* is for corresponding author)

KEYWORDS

Cyber Security, Investment, Cost Benefit Analysis, System Dynamics

INTRODUCTION

Cyber-attacks pose a major modern era threat to organisations that use networks (e.g., corporate networks and the Internet) to facilitate and improve business processes. The complexity of Internet vulnerability and increasing value of information stored in systems, make information security management a high-stake challenge to organizations. The objective of cyber-attacks may be identity theft, espionage, and disrupting operations of critical infrastructure (Behara et al. 2007, Knowles et al. 2015).

Defence against cyber-attacks requires substantial investment in cyber security resources. This complex problem with a large number of closely coupled variables associated with information security requires different analytical tools to support decisions on investment strategies. Not being able to effectively assess the consequences of information security investment decisions, leaves managers to speculate on the cost benefit. The assessment model needs to capture the complexities of the security decision while permitting a systematic exploration of alternative security options would serve as an invaluable aid to security managers (Behara et al. 2007, Bier 2014, Roumani et al. 2015).

System dynamics provide a tool for analysing complex situations. It helps to identify the causal loop amongst the variables of information target attractiveness and total number of attacks to analyse the effect of organizational security investments. The models can be simulated for different security management scenarios (Nazareth and Choi 2012, Behara et al. 2007).

CYBER SECURITY

Cyber-attacks on an organisation impact the performance and economics of an organization. The economics include profit margins, market capitalization and brand image of the organisation. Typical cyber-attacks include denial of services, malware, web-based attacks, phishing and malicious insiders (Mukhopadhyay et al. 2013, Roumani et al. 2015).

Information security has a life cycle that describes a cyber-attack. An attack by an adversary reaches for the information system of the organisation. A breach occurs when the attack penetrates and compromises the information system of the organisation. Recovery is performed to minimise the loss. Organizations resort to the use of technological devices in multiple levels of security defence to reduce the frequency and severity of a security breach (Mukhopadhyay et al. 2013, Behara et al. 2007). The cyber defence process includes Preventive, Detective and Corrective security perspectives. Effective defence depends on the selection of appropriate security management strategies from the different available options, each with different costs and potential benefits (Nazareth and Choi 2012).

COST BENEFIT ANALYSIS

Organisations must decide on a strategic level how much resources should be invested in Information Security to minimize the losses due to cyber-attacks. Cyber-risk disasters have a direct impact an organization in terms of loss on the bottom line, brand equity and market capitalization. Different methods for cost-benefit analysis that focus on the financial or managerial evaluation of security investments are available. Some commonly applied are Net present value (NPV), Return on Investment (ROI) and Analytic hierarchical process (AHP). These investments focus on the utility maximization principle to derive the optimal investment level under a limited number of constraining conditions. The problem is that these metrics approach treat information security as a static process with deterministic outcomes, which tends not to be true in the real world (Mukhopadhyay et al. 2013, Roumani et al. 2015).

Since information security is a complex system with qualitative and soft variables such as attacker intention, the organisation's defence, recovery processes, security policies, operating procedures, human behavioural factors, value of information sources, and intrinsic vulnerability of systems consequences of successful attacks, and other factors need to be addressed systemically. Cyber security measures may also only reduce the losses to an acceptable level, even with perfect protection. The relationships between these variables are circular, nonlinear and closely coupled. This complex situation requires a systemic approach, such as system dynamics, for analysing information system security issues and the impact of security investments (Nazareth and Choi 2012,Roumani et al. 2015, Behara et al. 2007, Mukhopadhyay et al. 2013).

SYSTEM DYNAMICS

Diverse 'hard' and 'soft' interrelated variables with dynamic relationships need to be investigated though simulation studies. This makes System Dynamics an appropriate tool to investigate strategy decisions and cost benefit analysis (Roumani et al. 2015, Nazareth and Choi 2012). System Dynamics is an iterative and interdisciplinary approach views problems holistically to identify the counterintuitive behaviour of the system due to policy based decisions. The methodology is a visual and mathematical modelling technique to study the dynamic behaviour of systems due to feedback and delays using simulation at high levels of abstraction. The soft variables ultimately become a hard (quantitative) representation of a particular problem expressed in precise mathematical way (Kasperek 2016, Sterman 2000, Meadows 2008).

A Causal Loop Diagram (CLD) represents the feedback structure of the dynamic system through capturing a hypothesis from stakeholder mental models on its dynamics and causes. The Stock and Flow Diagram (SFD) show the system structure that consists of physical processes, delays and stocks related to the dynamic behaviour in the system. Stock and flow variables are defined by a set of differential equations that can be solved to obtain the complex behaviour of a system over time. The SFD provides a clear overview of the whole system and all the relationships between the parameters (Sterman 2000, Roumani et al. 2015).

CYBER INVESTMENT COST BENEFIT ANALYSIS MODEL

The purpose of the System Dynamics model in this paper is to establish suitable cyber-security investment strategies for a public organisation. The investigations will focus on the ability of the organisation to defend its financial status against cyber-attacks. The cyber-defence capability is dependent on the organisation’s level of investment. The defended assets may be a website, list of customers, a strategic plan or account details. The System Dynamics model for information security management and investment is driven by security attacks on information assets and the efforts to reduce and recover the attacks. Cyber Security Investment provides a controllable variable in the model that directly or indirectly influences the other variables (Behara et al. 2007). The CLD in Figure 1 identifies the loops as the following:

1. Recovery Loop (Reinforcing 1). With increased Cyber Security Investment, the Recovery capability will increase, which will decrease the Cyber Incident Impact. Therefore the Financial Value of the organisation will improve that will provide more funds for Cyber Security Investment.
2. Prevention Loops (Reinforcing 2). With increased Cyber Security Investment the Threat Deterrence, Threat Detection and Attack Detection capability will increase, which will decrease the Cyber Incident Impact. Therefore the Financial Value of the organisation will improve that will provide more funds for Cyber Security Investment.
3. Vulnerability Loop (Reinforcing 3). With increased Cyber Security Investment the Cyber Vulnerability will increase, which will decrease the Number of Attacks and their effect on the Cyber Incident Impact. Therefore the Financial Value of the organisation will improve that will provide more funds for Cyber Security Investment.
4. Attractiveness Loop (Balancing 1). With increased Financial Value of the organisation, Target Attractiveness will increase, which will increase the Number of Attacks and their effect on the Cyber Incident Impact. Therefore the Financial Value of the organisation will be reduced that will limit funds for Cyber Security Investment.

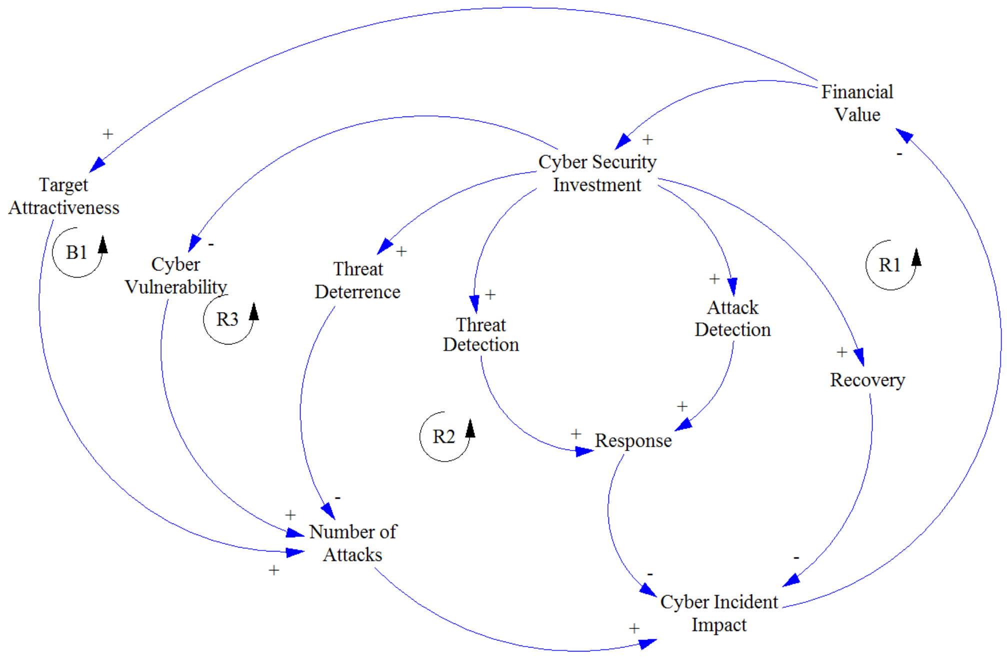

Figure 1: Causal Loop Diagram for Cyber Defence Investment

The CLD from Figure 1 is translated into a SFD that will facilitate simulation of different scenarios or policies, as seen in Figure 2. The model contains the following stocks that are affected by variables and constants over time:

1. Financial Value. The Financial Value is increased by a flow of Business Activity. This is assumed as constant and not affected by a cyber scenario. For this model the Financial Value is decreased by a flow affected by Cyber Incident Impact. An Attack Impact Ratio allows for setting the monetary value effect of a Cyber Attack.
2. Cyber Security Investment. The inflow of investment into cyber security is set by a ratio of the funds available in the organisation's Financial Value. The Cyber Security Investment is pulsed to realise an investment every four months. The Investment is also depreciated over time.
3. Cyber Vulnerabilities. The amount of Cyber Vulnerabilities existing in the ICT system of the organisation is increased by a constant rate, set to current levels experienced in real life. The Cyber Vulnerabilities are reduced by resolving them through capabilities established through investment. The Vulnerability Investment Ratio sets the number of vulnerabilities resolved per invested Rand.
4. Cyber Attacks. The number of Cyber Attacks experienced by an organisation is determined by the attractiveness to cyber criminals. The attractiveness is determined by the organisations' available Cyber Vulnerabilities Financial Value as well as investment into preventative measures. The existence of Cyber Attacks is reduced by recovery investments.

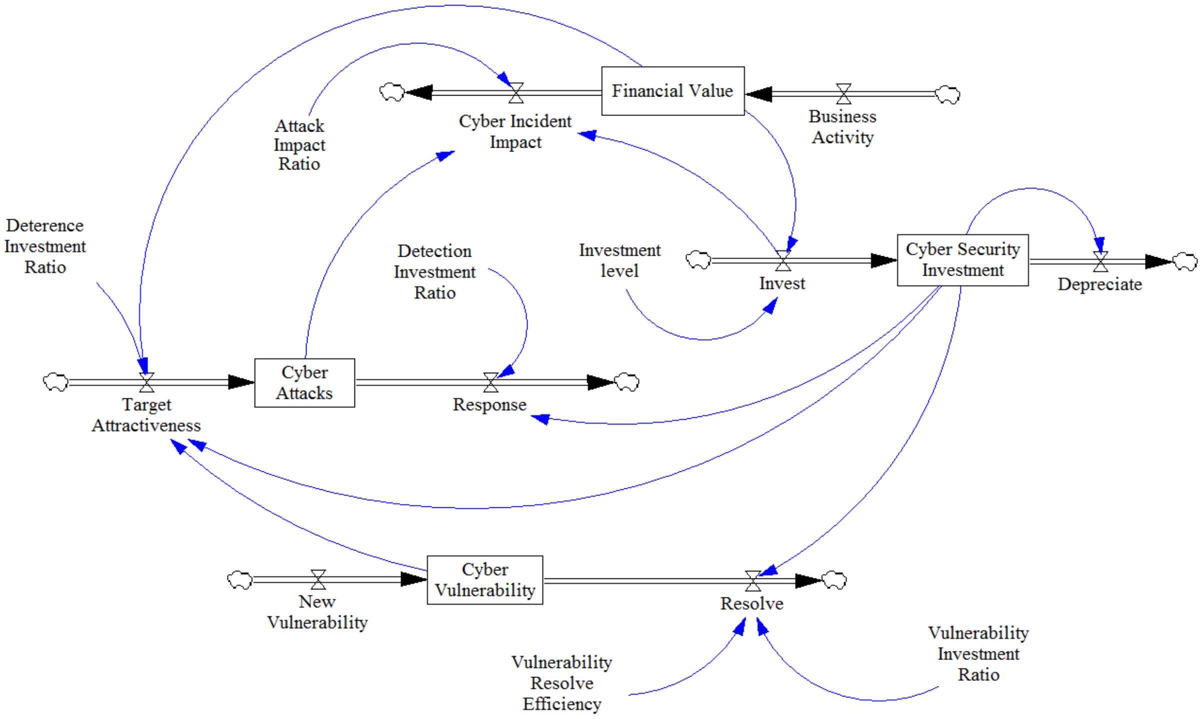

Figure 2: Stock and Flow Diagram for Cyber Defence Investment

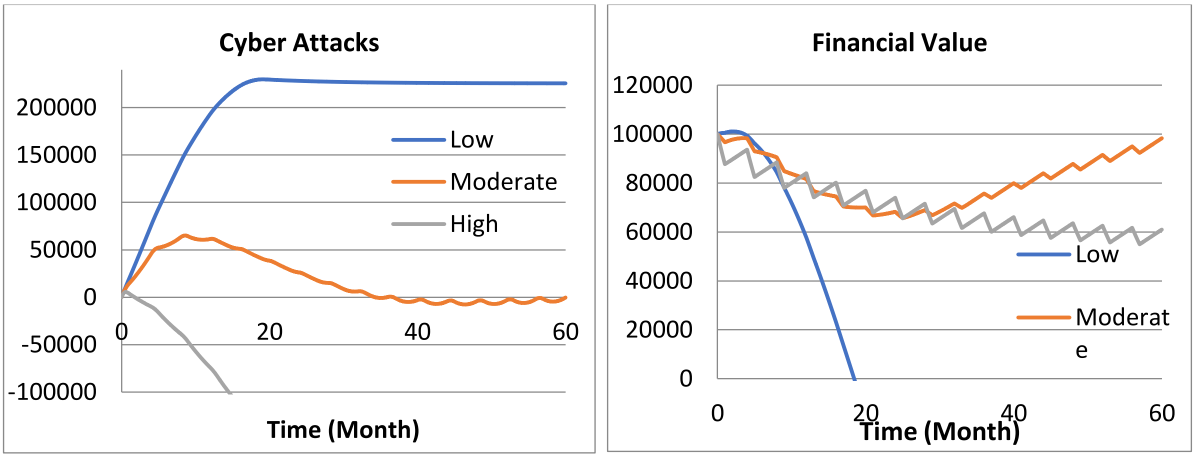

Figure 3: Preliminary Simulation Outputs

The simulation results from Figure 3 shows the comparative graphs for Cyber Attacks and Financial Value for low, moderate and high levels of Cyber Defence Investment. The graph is in line with what is to be expected of the system with the levels of Cyber Defence Investment. The high level of investment diminishes cyber risks while low investment levels results in a run-away situation. However, the Financial Value graph provides some counterintuitive behaviour. High levels of Cyber Defence Investment may deplete the organisations resources without real additional benefit, with a moderate investment level being more profitable in the long run. Also, a low investment level will be financially disastrous.

CONCLUSIONS

This is the initial attempt to develop and demonstrate the model to investigate the cost benefit of cyber security investments in an organisation. The results from the simulations show behaviour that is expected as well as some counterintuitive outcomes. This model will form the basis for continued improvement and validation. This model can be adapted to various organisations to investigate and optimise different investment strategies.

KEYWORDS

Cyber Security, Investment, Cost Benefit Analysis, System Dynamics

References

Bier, A.B., 2014. A Cognitive and Economic Decision Theory for Examining Cyber Defense Strategies. Sandia National Laboratories (Albuquerque, NM: Sandia Laboratories, 2014), at http://prod. sandia. gov/techlib/access-control. cgi/2014/140442. pdf.

Knowles, W., Prince, D., Hutchison, D., Disso, J.F.P. and Jones, K., 2015. A survey of cyber security management in industrial control systems. International journal of critical infrastructure protection, 9, pp.52-80.

Behara, R.S., Huang, C.D. and Hu, Q., 2007. A System Dynamics Model of Information Security Investments. In ECIS (pp. 1572-1583).

Roumani, M.A., Fung, C.C. and Choejey, P., 2015, June. Assessing economic impact due to cyber attacks with System Dynamics approach. In Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), 2015 12th International Conference on (pp. 1-6). IEEE.

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A. and Sadhukhan, S.K., 2013. Cyber-risk decision models: To insure IT or not?. Decision Support Systems, 56, pp.11-26.

Nazareth, D. and Choi, J., 2012. Information security management: a system dynamics approach.

Gordon, L. A., and Loeb, M. P. (2006) Budgeting process for information security expenditures, Communications of the ACM, 49, 1, 121-125.

Kasperek, D., Schenk, D., Kreimeyer, M., Maurer, M. and Lindemann, U., 2016. Structure-Based System Dynamics Analysis of Engineering Design Processes. Systems Engineering, 19(3), pp.278-298.

Sterman, J. D. 2000. Business Dynamics: Systems Thinking and Modeling for a Complex World. New York: Irwin/McGraw-Hill.

Meadows, D., 2008. Thinking in Systems: A Primer. Chelsea Green Publishing.