AMCIS: Estimating the Business Impact of Cyberattacks on Organizations

TREO Talk Paper

Akinori Kahata
The George Washington University
Cyber Security and Privacy Research Institute
akahata11@gwu.edu

Costis Toregas
The George Washington University
Cyber Security and Privacy Research Institute
toregas1@gwu.edu

Subhasish Dasgupta
The George Washington University
dasgupta@gwu.edu

Abstract

The importance of cybersecurity has increased in recent years and more and more organizations have to invest in cybersecurity. The problem organizations face is in determining how large an investment they need to make. A number of studies have tried to address this by using cybersecurity risk analysis and using it to help determine the amount of investment. In this research we propose an model for cybersecurity investment based on the business impact of cyberattacks. Our model focuses on the mechanism of cyberattacks and identifies the critical factors that have a significant impact on the organization's business. To improve the accuracy of the prediction, we continue to research the previous studies and gather more case studies to enhance and validate this model.

The overview of the model and estimation results

In our research we start by analyzing and evaluating the business impact of cyberattacks. To analyze the impact, we examine the current cybersecurity risk analysis literature, and postulate a sequence of cyberattack events and their effect on businesses as shown in Figure 1. Cyberattacks are identified as security incidents, security incidents have a business impact, and the business impact result in financial losses. Next, we examine what type of factors affect this sequence of events. Based on the general characteristics of each phase, three assumptions can be derived from figure 1, (a) lower cybersecurity preparedness has a higher likelihood of a significant security incident. (b) higher the dependence of an organization on information technology, bigger is the business interruption. (c) larger the organization size, more significant is the business interruption. Then, we identified the factors in Table 1 which can quantitatively represent the assumed relationship in the model. By using these factors, we propose a mathematical model which estimates the possible negative business impact of business interruption.

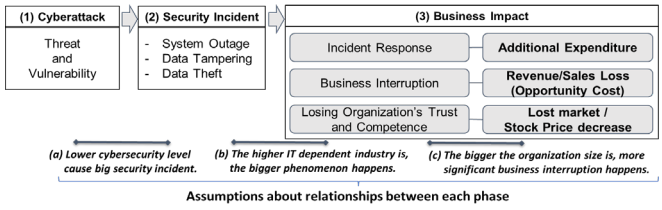

Figure. 1 The sequence of cyberattack cause business impact

Factor	Definition
Annual Revenue of Business: R	How much organization get money from business.
Type of Business Factor: T	IT dependency of each industry; calculate by I/O analysis (detail is next page).
Digitize Factor: D	How organization is digitized: Organizations' IT spending / Total revenue.
Cybersecurity Factor: CS	Strength of cybersecurity of the company: Cybersecurity maturity.
Normalization constant: k	Normalization factor for results: It can be optimized from results.

Table. 1 The factors of estimation equation

$$\textbf{\textit{Model: Business Impact of business interruption}} = k \cdot R \cdot T \cdot D \cdot CS$$

	Maersk
Cyberattacks	Ransomware (2017)
Business Impact (million USD)	300 (Profit)
R (million USD)	30945
Type of business	Water transportation
T (type of business factor)	0.000207
D (digitalization factor)	0.044
CS (cybersecurity factor)	0.85
Estimation of loss with best fit k (million USD)	55.8

Table. 2 The empirical evidence

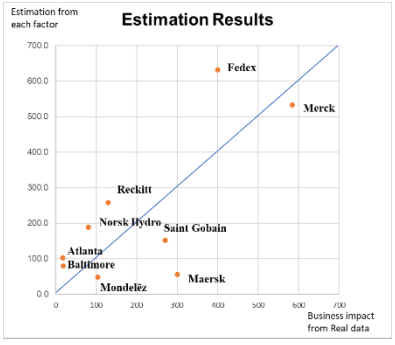

Figure. 2 Estimation results

Table.2 provides an example of fitting a real case to the model. Figure 2 shows the comparison of the estimation results and real data from annual reports of organizations.

We plan to enhance and validate this model using additional data and case studies.