A CONFIDENTIALITY, INTEGRITY, ACCESSIBILITY PRODUCTION FUNCTION FOR INFOSEC EVALUATION USING COBB DOUGLAS

Norman Pendegraft, College of Business and Economics, University of Idaho, Moscow ID 83843, 208-885-7157, norman@uidaho.edu

Mark Rounds, College of Business and Economics, University of Idaho, Moscow ID 83843, 208-885-4199, mrounds@uidaho.edu

ABSTACT

A production function is offered to describe the impact of changes in "production factors" (confidentiality, integrity, and accessibility) of an information system. Marginal analysis is conducted on several scenarios which suggests that the marginal value of the factors may behave very differently from one factor to another, and from one scenario to another. The model allows for concave and convex production functions consistent with the cases.

Keywords: infosec, value, simulation

BACKGROUND AND INTRODUCTION

This paper examines how the economic impact of a system breach should be modeled. In particular, it asks how the impact of different types of breeches should be evaluated. Verizon identifies a number of different attack types [16]. It seems that different types of attacks would have different economic impact. One of the most basic models of information security identifies three factors affecting value: confidentiality, integrity, or accessibility, the so-called CIA triad [13]. It is not clear that each of these has the same sort of impact on a system, nor it is clear that different systems have similar reactions to attacks of different types.

The paper continues a program of research examining the economics of information security from an ecological point of view. The program focuses on the fact that humans are a key element of infosec planning [12]. In earlier work [10], [11] etc. It was assumed that attackers were homogenous and that attacks were of one sort. Hence, the impact of attacks was modeled simply as a reduction of system value. One of the major problems in extending the program of research is how to correctly model the impact of attacks of different types on system value.

Here, we borrow the notion of a production function from economics [7]. A production function accepts as arguments the basic factors of production and calculates the resultant production. We create a simple production function model of system value, and allow that attacks may focus on only one of its factors.

We use the basic CIA model to identify those factors. The CIA model is widely used as a basic way of understanding infosec problems. To be sure, more complete models are available. For example, in 2004, NIST proposed a model with 33 constructs [15]. But, at an exploratory stage such as this work, we believe that simpler is better. While we limit our attention in this paper to CIA, there are other constructs mentioned in the literature. In 2004, NIST proposed a model with 33 constructs [15].

The remainder of the paper is organized as follows. First, we briefly summarize the CIA model. We then create a production function and show that it can model the scenarios. Then we use it to analyze several infosec scenarios. We conclude with a discussion of the results.

CIA MODEL

One basic model for understanding Infosec is the CIA model. The CIA model suggests that there are three major issues in computer security: Confidentiality, Integrity, and Accessibility. Confidentiality refers to restricting access to authorized individuals or processes. Espionage and credit card number theft are examples of confidentiality violations. Integrity refers to insuring that the data in the system is accurate. Failure of a system to ensure data consistency and changing the books to hide a theft are examples of integrity failures. Availability means that the system is accessible when needed. Denial of service attacks result in loss of availability.

As part of a program of research modeling the economics of infosec, we are interested in understanding the economics of attacks based on these three properties. Thus, our intent is to understand the marginal impact on system value of changes in C, I, and A. This understanding will help us build better models.

VALUE AS A PRODUCTION FUNCTION

A production function is an economic model of value created in a firm as a function of the inputs, traditionally labor and capital. Here we look at factors impacted by loss of confidentiality, integrity, and accessibility. Thus, we look for a production function V

$$V = V(C, I, A) \tag{1}$$

To simplify matters we suggest that C and I be limited to the interval [0,1]. C=0 implying public information, and I=0 implies random data with no value. Similarly, C=1 implies perfect security with data known only to authorized users, I=1 implies data that is completely correct.

Clearly first partial derivatives should be positive since the factors are all good things and more is better. However, signs of second partials are less clear. The second derivative tells us whether the Value of the system increases at an increasing rate (positive) or increases at a decreasing rate (negative). For example, the second partial of quantity is presumably negative due to declining marginal value. However, in a growth stage of social media, it may be that it is positive: the more members you have the more connections an additional member can make, and hence the second partial of quantity may be positive over a broad range of values.

There are several functions commonly used to model production functions.[7] . Because of its versatility, we examine a power function $f(x)=a\ x^{b}$. This function has the advantage that by simply varying b, we can create functions which are convex and others that are concave. When b>1 it is convex; when b<1 it is concave.

One of the most widely used production functions in economic analysis is the Cobb-Douglass function: $F(L,C)=L^{\alpha}C^{\beta}$ where $0<\alpha, \beta$. It is commonly assumed that $\alpha+\beta=1$ which gives some nice results. However, there is nothing inherent in the model that requires this constraint. We propose to use a multiplicative power function form of the Cobb Doulas model, with simple constraints.

$$V(C, I, A) = C^{\alpha}\ I^{\beta}\ A^{\gamma} \tag{2}$$

where

C is the level of privacy, 0<C<1
I is the integrity or quality, 0<I<1, and
A is the accessibility or quantity of data, 0<A, and
α,β, and $\gamma > 0$

We believe that attacks on the quantity of data available serves as a proxy for accessibility because accessibility operates by reducing the amount of data that is accessible.

Note that

$$\frac{\partial \mathrm{V}}{\partial \mathrm{C}} = \frac{\alpha\, \mathrm{V}}{\mathrm{C}} \tag{3}$$

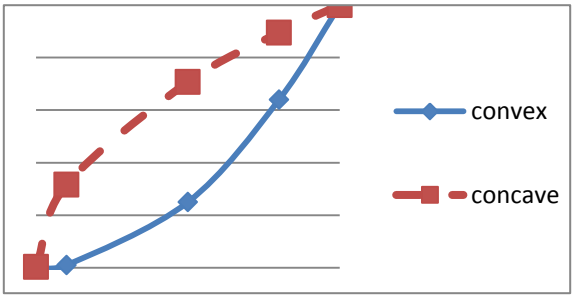
and that

$$\frac{\partial^2 V}{\partial C^2} = \frac{\alpha^2 V}{C^2} - \frac{\alpha V}{C^2} = \frac{\alpha V}{C^2}(\alpha - 1) \quad (4)$$

Thus, when $\alpha<1$ the second partial is negative and when $\alpha>1$ the second partial is positive as claimed. Similar results hold for the other two factors.

The graph in Figure 1 illustrates the general shape of the curves in questions. Both curves have positive first derivatives. The dashed curve has a negative second derivative and the solid curve has a positive second derivative.

FIGURE 1



One of the questions of interest to modelers is whether to use a concave or convex function to model response to attacks. A negative second partial (concave) is consistent with marginally decreasing economic value or with risk-averse behavior in decision making, and the positive (convex) curve is consistent with marginally increasing values or risk seeking behavior. Here we are looking at losses rather than gains. Prospect theory [5] suggests that many people are risk averse over gains and risk seeking over losses. Thus, we believe that a positive second partial (convex curve) may make sense here.

THE CASES

One of the questions of interest to us as modelers is: is the production function concave or convex with respect to these factors. In many economic systems, there are decreasing returns to scale which argues in favor of a concave function. But as noted above, many people seem to have convex utilities functions with respect to loss. Hence, we examined several security problems and found examples were the curve seems to be convex and others where is seems to be concave. Since we are here merely trying to show existence of such cases, we postpone more detailed examination of the literature to look for patterns in these cases.

In a classic case of loss of confidentiality, US Navy codebreakers in 1942 were able to decode a fraction (less than 5%) of Japanese naval radio traffic. Nonetheless, they were able to deduce the date and direction of attack for the invasion of Midway. The information resulted in a major US Naval victory [9]. Thus, we conclude that V (for the defender, here the Japanese) was convex with respect to C.

In a recent case, Facebook experienced a serious loss of confidentiality. Nonetheless, there seemed to be little reaction among users. Hence, we conclude that in this case V is concave with respect to C. [8]

Embezzlement is a $100 million dollar problem involving a reduction in Integrity. Usually embezzlement involves falsifying financial records to hide a theft. A small change in the data can hide a substantial theft of funds [6]. Here is seems V is convex with respect to I.

Web defacement is also an attack on data integrity. It appears that many web defacement attacks have little if any long term impact. For example, a 2014 report on defacement attacks on the World Cup web site seems to have had little impact, despite a series of over 100 attacks [17]. This suggest to us a concave response to I.

In another classic case, the Bank of New York experienced a short (2 hour) computer failure in 1985 which required that it borrow over $20 billion over night at a rate of 7.5% which cost the bank around $5 million.[1],[2]. Here it appears that V is convex as a function of accessibility.

A recent survey [4] indicates that Distributed Denial of Service (DDoS) attacks are common with over 90% of respondents reporting a DDoS in the previous year. Despite the numbers and the significant cost, there was no report of a company failing or incurring major damage. So, it appears that a fairly large attack (6-24 hours) resulted in limited long term damage. Thus, we conclude that this suggests that Value is concave with respect to A.

Facebook recently announced that their growth had slowed substantially. Markets reacted very negatively suggested that investors viewed even a small decrease in the growth rate of users is a serious concern. Hence, we conclude that the value is convex with respect to quantity of data. This example also suggests to us that quantity of data is related to accessibility [14].

SIMULATION

We built a simple continuous event simulation with IThink [3] illustrated in Figure 2. Due to space limitation, for this paper we ran only a few simulations. Figure 3 illustrates the base case in which attacks of all three types are equal as are security allocations and $\beta=1$. This results in Value being constant over time. Figure 4 illustrates a case in which the total attacks is the same, but there are more type I attacks than the others. Value declines over time. Figure 5 illustrates a case in which attacks are the same as in Figure 4 but security is also skewed toward type I.

Figure 6 shows sensitivity to the exponents in the power function. Here the number of I attacks varies (keeping total attacks constant) with $\beta=1.7$ and security constant and balanced. Note that with a low number of I attacks value increases. But, as the number increases, value declines rapidly.

DISCUSSION

We suggest that a generalized version of the Cobb Douglas production function model may be used to model the value of information systems under attack. We find that there are examples in which the exponents are greater than one and other examples in which the exponents are less than one. The proposed model will allow future researchers building simulation or analytical models of information system under attack to build richer model in which different types of attack may be modeled. Each of the different types of attack may be modeled to have different marginal impact on the system depending on the specifics of the industry and attack vehicle being considered.

The simulation illustrates that it is capable of treating different types of attack differently. It further offers guidance to policy makers to ask question about their own systems. What are the marginal impacts of attacks? It would seem that attacks against factors with convex impact on the value function would be of greater importance. If there are two, then the question is which is steeper? None of these are easy questions, but the model offers a framework for structuring such questions.

FIGURE 2

IThink Model

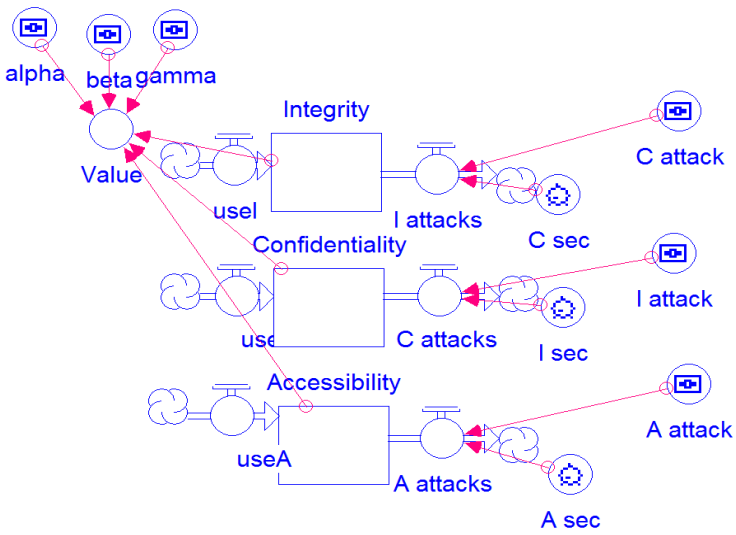


FIGURE 3

Value Base Case

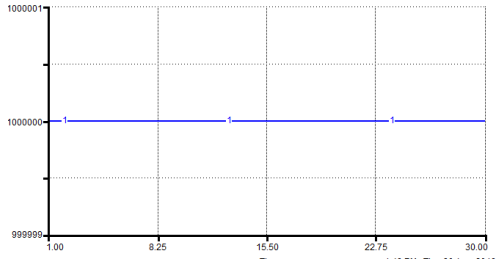


FIGURE 4

Value, Biased Attack

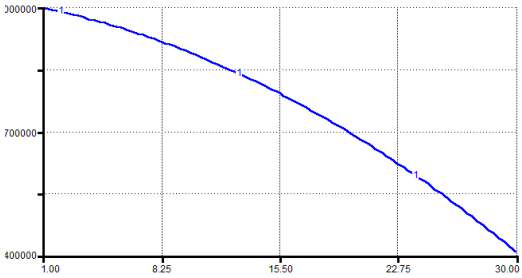


FIGURE 5

Value: Security matches biased attack

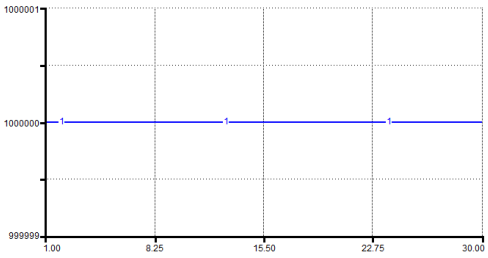
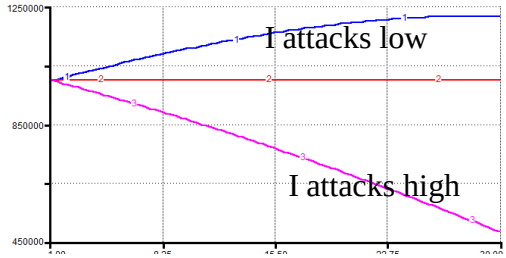


FIGURE 6

Value: High β, I attacks vary



REFERENCES

[1] Berry, J. (1985, Dec 13). Computer Snarled N.Y. Bank. The Washington Post.
[2] Ennis, H., & Price, D. (2015). Discount Window Lending: Policy Trade-offs and the 1985 BoNY Computer Failure. Federal Reserve Bank of Richmond.
[3] High Performance Systems. (n.d.). IThink. Lebanon, NH.
[4] Incapsula. (2014). Incapsula Survey: What DDos Attacks Really Cost Businesses. Retrieved from http://lp.incapsula.com/rs/incapsulainc/images/eBook%20-%20DDoS%20Impact%20Survey.pdf
[5] Kahneman, D., & Tversky, A. (1979). Prospect Theory: An analysis of decision under risk. Econometrica, 263-292.
[6] Karpp, D. (2016). The 2016 Hiscox Embezzlement Study. Hiscox.
[7] Keat, P., & Young, P. (n.d.). Managerial Economics, 5th ed. Pearson.
[8] Martin, R. (2018, July 9). More Facebook Vulnerabilities Come to Light...But does it matter? Retrieved from InvestorPlace: https://investorplace.com/2018/07/more-facebook-vulnerabilities-come-to-light-but-does-it-matter/
[9] Munson, M. (2016). The Battle of Midway: The complete intelligence story. War on the Rocks.
[10] Pendegraft, N., & Rounds, M. (2007). A Simulation Model of IS Security. International Journal of Information Security and Privacy, 1.
[11] Rounds, M., Pendegraft, N., & Taylor, C. (2007). The Ecology of IS Security: A Research Agenda. Information Resources Management Association International Meeting. Vancouver, B.C.
[12] Saltzer, J., & Schrodeder, M. (1975). The Protection of information in computer systems. Proceedings of the IEEE 63#9, 1278-1308.
[13] Samonas, S., & Coss, D. (2014). The CIA Strikes Back: redefining Confidentiality, Integrity and Availability in Security. Journal of Information System Security, 21-45.
[14] Seetharaman, D. (2018, July 25). Facebook Shares Tumble as Growth Outlook Darken. Wall Street Journal.
[15] Stoneburger, G.; Hayden, C.; Feringa, A.;NIST. (2004). Engineering Principles of Information Technology Security. U.S. Department of Commerce.
[16] Verizon. (2018). 2018 Data Breech Investigations Report. Retrieved from https://www.verizonenterprise.com/verizon-insights-lab/dbir/
[17] Vinton, K. (2014, Jun 18). Hacktivist Group Anonymous Targets World Cup. Retrieved from Forbes: https://www.forbes.com/sites/katevinton/2014/06/18/hacktivist-group-anonymous-targets-world-cup/#5e2ba053238b