Journal of Information Security, 2016, 7, 281-290
http://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Cybersecurity: Integrating Information into the Microeconomics of the Consumer and the Firm

Scott Farrow

Department of Economics, UMBC, Baltimore, USA
Email: Farrow@umbc.edu

How to cite this paper: Farrow, S. (2016) Cybersecurity: Integrating Information into the Microeconomics of the Consumer and the Firm. *Journal of Information Security*, **7**, 281-290.
http://dx.doi.org/10.4236/jis.2016.75023

Received: July 7, 2016
Accepted: August 27, 2016
Published: August 30, 2016

Abstract

The connectivity of information has changed many things but not the way economists model consumers, firms and government. Information is here newly modeled as a fundamental element of microeconomic choices and utility, cost and tax functions. The results are more clearly defined metrics for losses due to cyber breaches or productivity gains from cyber investments. The integration of information into standard microeconomics also allows use of econometric and other tools to analyze the empirics of the consumer and the firm. In particular, the results identify ways in which losses in the Gordon and Loeb [1] model can be specified in more detail.

Keywords

Microeconomics, Utility, Cost, Cyber Losses

1. Introduction

Capital and labor are the time honored categories for production inputs which are transformed into marketable goods and services. But the economy is more virtual now with information occupying a central place in economic activity. Economics has primarily dealt with information as an issue in information gathering for decision-making under uncertainty as in Bikhchandani, Hirshleifer and Riley [2]. A major area of application includes labor market signaling as in Rogerson, Shimer and Wright [3]. However, maintaining the abstraction that information is an imprecise signal for a decision or simply changes the quality or quantity of (computer) capital does not capture the many ways that information itself is an input into production. Shutting down a website and a consumer's virtual access to a business is damaging; intellectual property and personal identity are stolen virtually, production processes can be controlled by or destroyed by changes in the information running the machines. Motivated by issues in cybersecurity, this note investigates the ways information alters fundamental structures of the consumer, firm and government. Analyzing those structures more clearly identifies microeconomic definitions of cybersecurity losses even in the absence of a decision involving uncertainty.

Gordon and Loeb [1] obtained significant insight by abstracting cyber information sets from the remainder of the economic activity of the firm or organization. Information sets were interpreted broadly; potentially including data sets, websites, accounting information, algorithms, intellectual property, electronic communications and so on. In their model and extensions as in Farrow and Szanton [4], the effect of a cyber information breach results in a conditional loss, L, to the firm. The loss is a part of an expected value objective function where probabilities of loss are modeled separately. In Gordon, Loeb, Lucyshyn and Zhou [GLLZ, [5]], the losses include external effects beyond the firm. There is however, value in re-integrating their sparsely defined conditional loss into the more detailed but standard microeconomic modeling of the firm, the consumer, and government. Such reintegration facilitates the decomposition of losses due to a breach, the differentiation of types of attacks, and the distinction between what GL refer to as private and external costs of an attack[1].

Microeconomics builds from an individual consumer and firm up to the market and general equilibrium levels. However, research on cyber losses to both consumers and firms has taken a more ad-hoc approach. Prior research seems to have taken two alternative approaches. One approach in the information technology literature is to develop taxonomies of types of attacks, potentially distinguished by their method of attack or the outcome as in Undercofer, *et al.* [8]. A second approach has focused on cost categories. Detica [9] focused on the costs associated with various stages of cyber-attacks, identifying categories of costs in anticipation, in consequence, in response, and indirect costs. Anderson, *et al.* [7] organize their cost analysis using direct, indirect, and defensive costs with the cost to society being the sum of these categories.

In contrast to the existing cyber focused work, the standard sequence of firm and consumer modeling is developed here in order to explicitly identify the pathways losses can occur. Such a delineation may encourage more detailed empirical modeling given the methodologies already developed for analyzing microeconomic structures. While the focus here is on the mechanism of losses due to some type of cyber activity, the dominant impact of cyber activity has been gains through many of the same mechanisms capable of generating losses.

2. Modeling Information as an Input

2.1. Information and the Consumer

Begin with the consumer who, for example, can be directly affected by breaches of Personal Identifying Information (PII) and whose choices create demand for a firm's

[1] The economics literature on crime typically defines attacks as externalities as there is no voluntary exchange (Levinson [6]). Most cyber breaches can be viewed as types of crime enabled by computers or that are uniquely possible with computers (Anderson *et al.* [7]). The crime literature further debates whether "thieves" have standing for costs and benefits with the usual but not universal conclusion that they do not. This is especially important for issues such as intellectual property or international cybercrime.

product.

A deterministic model identifies goods Q_i that may have characteristics dependent on embedded cyber information and capabilities, $\boldsymbol{I}$, as is common with many consumer goods. Furthermore, transactions are facilitated by cyber information and processes typically embedded in computers, phones or other devices and linked to the internet. Consequently the good itself and its purchase is partially defined by cyber information, $Q(\boldsymbol{I})$. Prices, P_i, are here assumed parametric in the budget constraint, Y such that:

Max Utility $\left(Q_1(\boldsymbol{I}), Q_2(\boldsymbol{I}), Q_3(\boldsymbol{I}), \cdots, Q_n(\boldsymbol{I})\right)$

w.r.t. Q_i

Subject to: $\sum_1^n P_i(\boldsymbol{I}) Q(\boldsymbol{I}) = Y$

Cyber breaches can then affect the consumer's utility through various pathways. The direct theft from a consumer, perhaps from the loss of PII, can be modeled as a discrete decline in income[2], $Y(\boldsymbol{I})$. More complexly, consider that characteristics of differentiated goods are identified both by their embedded use of cyber information through software, displays, controls and so on while the transaction cost and purchase context is also influenced by cyber information. To the extent that there are changes in the cyber information embedded in the good, prices[3], or income then the consumer's demand, $Q_i(\boldsymbol{I}) = f(P_i(\boldsymbol{I}), P_j(\boldsymbol{I}), Y(\boldsymbol{I}), \boldsymbol{I})$, changes. The total derivative of demand, Equation (1), thus identifies specific chains or pathways of effects from changes in information to observable quantities based on consumer behavior.

$$\mathrm{d}Q(\boldsymbol{I}) = \frac{\partial f}{\partial P_i}\frac{\partial P_i}{\partial \boldsymbol{I}}\mathrm{d}\boldsymbol{I} + \frac{\partial f}{\partial P_j}\frac{\partial P_j}{\partial \boldsymbol{I}}\mathrm{d}\boldsymbol{I} + \cdots + \frac{\partial f}{\partial Y}\frac{\partial Y}{\partial \boldsymbol{I}} + \frac{\partial Q}{\partial \boldsymbol{I}}\mathrm{d}\boldsymbol{I} \tag{1}$$

The consumer's problem can also be written in terms of household production where household labor and purchased inputs yield household output as in Becker [10] or Gronau and Hammermesh [11]. For instance, loss of an individual's time to re-establish identity or time involved with personal malware leads one to a household production model where time has a shadow price primarily measured by household labor. While not fully developing that model here, household labor can be affected, both positively and negatively, by cyber information, $H(I)$. Other household inputs such as electricity and water are information dependent, HE($\boldsymbol{I}$) and HW($\boldsymbol{I}$), and are of concern due to potential cyber-physical infrastructure damage.

An information set (or just information) augmented consumer model thus captures: a) changes due to loss of income, b) costs associated with household production including unpaid time, c) changes in the quality of goods including the process of obtaining them, and d) potential changes in the utility function itself. For instance, the result of stolen PII from a retailer may involve changes in utility (and associated monetized value of that utility loss) reflected in a tighter budget constraint, having to spend

[2] As governments heavily depend on income taxes; such taxes could be modeled as depending on income and cyber information. For simplicity, such tax modeling is omitted here but included in the description of the firm.

[3] Note that to the extent effects are mediated through market price changes, then there can be usual income and substitution effects.

time and other household inputs to restore their identity and changing their demand for products from that source or similar sources. In the latter case, there could be a public bad of decreased quality across multiple goods, a topic investigated in more detail below. Alternatively, the primary effect of cyber information change can be positive for the consumer (as it typically has been from non-criminal use of cyber information).

2.2. Information in the Firm and the Government

Firms are linked to consumers via the market demand (or inverse demand) function, shown above to depend on cyber information and upon aggregation across consumers. But the firm's output also depends on its production function, f. Begin with a classical production function in which output, Q, is a function of capital and labor, $f(K, L)$. Consideration is given first to the situation where no network or other externalities exist. The role of (ostensibly) internal cyber information, I, can be modeled as both a stand-alone input and an intermediate input embedded in and affecting the productivity of K and L. The usefulness of considering the stand-alone portion occurs for instance, when considering theft of PII or intellectual property. The capital and labor within the firm would still operate with the same productivity, but a loss occurs. Examples of an effect mediated through capital and labor is malware which can affect the productivity of both inputs. Within a firm, initially augment a production function as $Q(I) = f(L(I), K(I), I)$. Cyber security from the firm's perspective, absent externalities, is to consider how the production process is damaged if the I input is compromised, as from attacks which may affect confidentiality, integrity, authenticity, availability to users and so on. Further, I may affect the very definition of the output such that differentiated products may viewed by the consumer differently if they are secure or not.

Now consider the role of public goods (or bads) which is the mechanism through which externalities occur. Current production typically depends not only on the firm's own cyber information input, I, but also that of the external cyber system to which it is connected, $\boldsymbol{I}$, comprised at least of all the linkages the firm uses on the internet or more indirect effects as through communications, control of utilities, and so on. Such a public good input may affect production directly or indirectly through other inputs. For instance, infrastructure damage to I may both impair the firm's internal cyber information input as well as capital. Further, an attack over the internet may result in technological adaptation or response by the firm. While this could be considered an entirely new production function, here such responsive actions are modeled as direct shifts in output or shifts mediated through capital and labor with resulting implications for costs. A production function including both types of internal and external cyber information can then be written as $Q(I, \boldsymbol{I}) = f(L(I, \boldsymbol{I}), K(I, \boldsymbol{I}), I(\boldsymbol{I}), \boldsymbol{I})$. There is also the standard cost function—representing the minimum cost of producing a level of output given the production function and input prices—here shortened to focus on the role of information as $C(I, \boldsymbol{I})$.

The final element affected by cyber information is demand for the firm's product which, in perfect competition, is pre-determined at the firm level but jointly determined by supply and demand at the market level. At the market level, the internal cyber information is presumably so small as to not affect the price, but an external impact of cyber information may exist at the market level. Hence a competitive market price depends on external cyber information $P(\boldsymbol{I})$. For an imperfectly competitive firm the price is a function of the firm's marginal revenue and marginal cost and, given the prominent role of internet sales and communication, hence characterized as a function of both the internal and external cyber information, $P(I, \boldsymbol{I})$.

Consequently the pre-tax profit function for a firm can be written as $\pi(I, \boldsymbol{I}) = P(I, \boldsymbol{I})$ $Q(I, \boldsymbol{I}) - C(Q(I, \boldsymbol{I}))$ with some of the internal cyber information possibly irrelevant to a competitive firm. However, government and industry also interact in a variety of ways. The production function itself may be constrained by various regulatory policies. Changes in such policies can result in a changed production function perhaps but not necessarily related to cyber information. More directly, a number of taxes transfer money from industry (and the consumer) to Government. The bi-directional impact of cyber information on taxes and tax revenue is here modeled by a tax on profits, $\tau(\pi(I, \boldsymbol{I}))$, although the focus below will be on the effect of the external effects. Including the tax effect allows for losses in government revenue potentially due to loss of intellectual property, or gains if government imposes taxes or fines on a firm due to cyber information breaches and or other actions.

Define the total potential private supply side loss due to information as the total derivative of the profit function:

$$\begin{aligned} \mathrm{d}\pi\left(I, \boldsymbol{I}\right) &= \frac{\partial \pi}{\partial I}\mathrm{d}I + \frac{\partial \pi}{\partial \boldsymbol{I}}\mathrm{d}\boldsymbol{I} \\ &= \left[\frac{\partial P}{\partial I}Q + P\frac{\partial Q}{\partial I} - \frac{\partial C}{\partial Q}\frac{\partial Q}{\partial I}\mathrm{d}I - \tau\frac{\partial \pi}{\partial I}\mathrm{d}I\right] + \left[\frac{\partial P}{\partial \boldsymbol{I}}Q + P\frac{\partial Q}{\partial \boldsymbol{I}} - \frac{\partial C}{\partial Q}\frac{\partial Q}{\partial \boldsymbol{I}}\mathrm{d}\boldsymbol{I} - \tau\frac{\partial \pi}{\partial \boldsymbol{I}}\mathrm{d}\boldsymbol{I}\right] \end{aligned} \tag{2}$$

Each term in Equation (2) represents a pathway through which changes in information can affect profit where the key pathways are through price, quantity, cost, and taxes. One may also ask, what about financial dimensions of firms such as stock market prices, net worth, and borrowing costs? These financial dimensions are considered here as derivative of the profit position of the firm. If profit expectations decline due to cyber breaches, that decline is expected to affect the financial condition of the firm including its forecast net worth, stock value and so on. Such links could be analyzed through the impact on the profit function as in Campbell *et al.* [12].

Finally, Government is potentially affected by cyber information both through its own production and through its financing from taxes on firms and consumers. Regarding government production, the same pathways occur as with private firms with the caveat that neither costs are assumed to be minimized nor is social profit maximized. Hence government output is affected by both its internal and external cyber information, $\mathrm{G}(I,\boldsymbol{I})$ through the processes similar to those above.

3. Defining Losses

3.1. Deterministic Losses

The literature on cyber costs uses various loss categories such as direct, indirect, defensive and so on. Such categories may be informative for particular data sets but are not economically well defined terms. Table 1 presents several candidate classifications based on widely used language from accounting, microeconomics and macroeconomics.

The accounting terms "direct" and "indirect" have little classification power as cyber information losses (or gains) are spread across both production and "back office" processes which is central to the accounting definition. The distinction between private, external, and pecuniary effects from microeconomics has some classification power, although cyber losses are almost always initiated through an externality; they are not the result of a voluntary exchange. Like the spread of disease however, there can be an initial loss which is spread as an additional externality, as through malware. Pecuniary externalities can exist as markets are affected. Finally, macroeconomic terms have some classification power by incorporating the production and market linkages across industries. For instance, the banking sector may incur losses from re-issuing cards as the result of a PII data breach in another industry. In short, the macroeconomics reminds us of industry interactions such as when an information loss in industry j causes a change in industry i. That change may operate through the price mechanism, the legal system or other mechanisms. Similarly, interactions may occur through the endogeneity of the household sector as with induced effects. Finally, there may be political economic effects through government, including regulation.

The modeling of Section 2 allows loss definitions to depend on the partial derivatives that are affected. Consequently, direct effects are here taken to be the partial derivatives in the consumer, firm, and government problems that are not mediated through market prices or through non-market responses such as regulation. Secondary (or indirect including induced) effects are those responses mediated through the market. The direct effects

Table 1. Loss categories from different professional framings.

Professional Framing	Categories and Meaning
Accounting: direct and indirect	Direct associated with production or identifiable cost sector, compared with widely spread indirect costs.
Microeconomics: private and external	Private: the result of voluntary exchanges while external effects are involuntarily incurred (positively or negatively) by third parties. Pecuniary externalities are third party effects mediated through market prices.
Macroeconomics: direct, indirect, induced	Whether at the industry level or firm level, direct output effects are identified with a change in output of a specific firm or industry while indirect effects are those from industry production or market linkages. Induced effects occur when households are endogenous to the system and expand or contract activity as part of a general equilibrium system. Secondary effects can be either or both of indirect or induced.

identified above are then the partial derivatives: $\partial Y/\partial \mathbf{I}, \partial Q/\partial \mathbf{I}, \partial HL(\mathbf{I})/\partial \mathbf{I}, \partial HX(\mathbf{I})/\partial \mathbf{I}$ for the consumer and $\partial Q/\partial I, \partial C/\partial I, \partial I/\partial \mathbf{I}, \partial Q/\partial \mathbf{I}, \partial C/\partial \mathbf{I}$ for the firm, noting that $\partial \pi/\partial \mathbf{I}$ (associated with taxation) is affected by both direct and indirect changes to be further defined below. These direct effects are identified by the economic actor and the mechanism of impact rather than whether the actor chooses, for instance, to alter their production function via changes in software, capital, labor or some other aspect. Consequently, in the case of PII, both damages incurred by a consumer and monitoring or re-issue costs in the financial sector would be deemed direct, while possible changes in interest rates charged would be indirect as that latter is mediated through the market mechanism.

The secondary or indirect effects are then $\partial P_i/\partial I, \partial P_j/\partial I, \partial P_i/\partial \mathbf{I}, \partial P_j/\partial \mathbf{I}, \partial G/\partial I, \partial G/\partial \mathbf{I}$ reflecting the interactions through the marketplace or regulation.

Illustrative components of loss from two types of cyber breaches, payment card fraud and intellectual property, are presented in **Figure 1** for direct costs and **Figure 2** for indirect costs. The type of cyber breach is identified on the left with arrows leading to categories of effects—the partial derivatives—and a partial linkage to categories identified in Anderson, *et al.* [7].

This enumeration of core pathways for cost in standard economic terms has the potential to identify costs typically ignored, such as potentially positive or negative price effects, and to provide a structure in which to identify other pathways and elements of loss. Economists are familiar with estimating elements of consumer demand and firm costs and production. The proposed framing of losses into a standard economic framework may facilitate the transition of empirical methodologies to cyber loss estimation and estimation of the partial derivatives based on data.

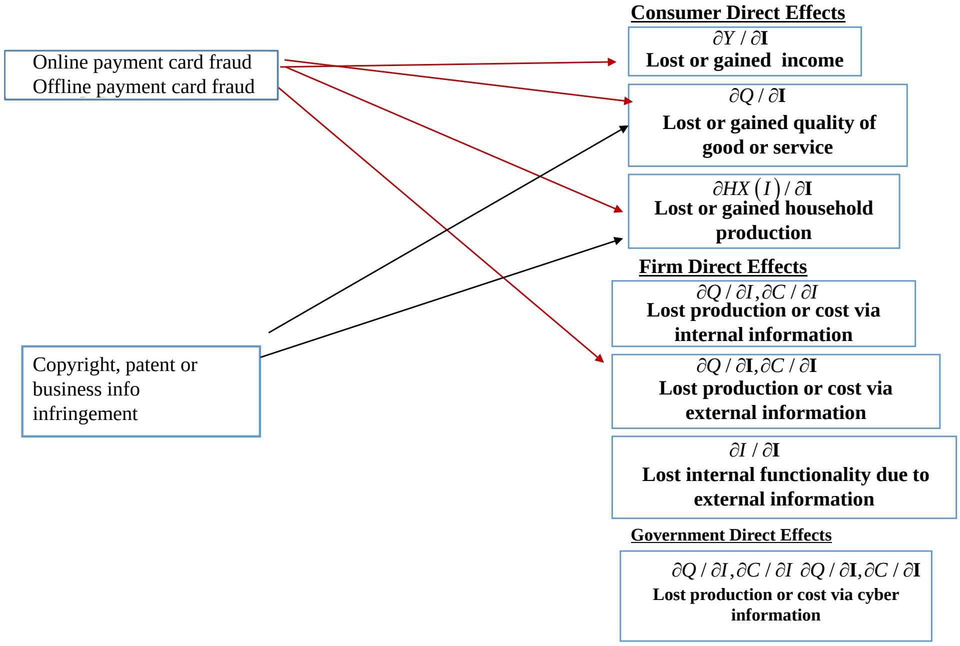
Online payment card fraud
Offline payment card fraud
Copyright, patent or business info infringement
Consumer Direct Effects
∂Y / ∂I
Lost or gained income
∂Q / ∂I
Lost or gained quality of good or service
∂HX (I) / ∂I
Lost or gained household production
Firm Direct Effects
∂Q / ∂I, ∂C / ∂I
Lost production or cost via internal information
∂Q / ∂I, ∂C / ∂I
Lost production or cost via external information
∂I / ∂I
Lost internal functionality due to external information
Government Direct Effects
∂Q / ∂I, ∂C / ∂I ∂Q / ∂I, ∂C / ∂I
Lost production or cost via cyber information

Figure 1. Direct effects of illustrative cyber online fraud and intellectual property breach.

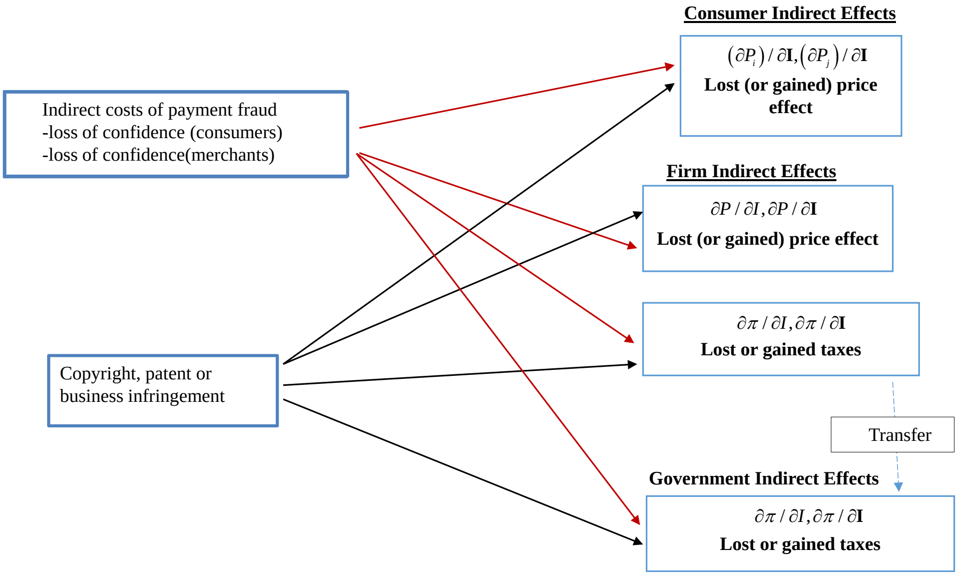
Consumer Indirect Effects
$(\partial P_i)/\partial \mathbf{I}, (\partial P_j)/\partial \mathbf{I}$
Lost (or gained) price effect
Indirect costs of payment fraud
-loss of confidence (consumers)
-loss of confidence(merchants)
Firm Indirect Effects
$\partial P/\partial I, \partial P/\partial \mathbf{I}$
Lost (or gained) price effect
$\partial \pi/\partial I, \partial \pi/\partial \mathbf{I}$
Lost or gained taxes
Copyright, patent or business infringement
Transfer
Government Indirect Effects
$\partial \pi/\partial I, \partial \pi/\partial \mathbf{I}$
Lost or gained taxes

Figure 2. Indirect effects of illustrative cyber payment fraud or intellectual property breach.

3.2. Some Effects of Uncertainty in Defining Losses

The loss estimates in Gordon and Loeb [1] and Gordon, Loeb, Lucyshyn and Zhou [5] are part of the objective function where the expected net benefit of a cyber investment is maximized. The losses, elaborated upon above, are the conditional losses where cyber security investment expenditures affect the probability of a successful attack. Continuing to focus on losses, the model of the consumer and firm has long been extended to conditions with uncertainty based on the expected utility model and more recently, non-expected utility models.

A natural extension to expected value optimization is expected utility maximization. To the extent that losses are potentially large so that a significant gamble is involved, then some risk aversion may be present as in Eeckhoudt, Gollier and Schlesinger [13]. Numerous methods exist in economics and decision analysis to elicit utility functions subject however, to the more restrictive assumptions that imply cardinal instead of ordinal utility (e.g. [14] [15]). The concern by some firms for a reputational effect from a cyber breach or intellectual property theft may well warrant extending the model of losses to expected utility instead of expected value. Consideration of risk aversion leads naturally to consideration of insurance as a risk management strategy in addition to prevention which has indeed occurred.

However, the descriptive validity of the expected utility model is being questioned by behavioral economists and psychologists with a rich and rapidly evolving literature on consumer and firm behavior under uncertainty (Della Vigna, [16]). That literature identifies a number of outcome anomalies such as the importance of reference points and asymmetric treatment of gains and losses as well as more complex treatment of probability than in the expected utility model. An analyst seeking a descriptive model of cyber losses may wish to include consideration of such factors. In empirical practice, such consideration can simply involve a different specification of an assumed utility function as compared in Farrow and Scott [17].

Although this note has focused on defining conditional losses, cyber investments are often modeled as directly affecting the probability of the loss. Given that framework, the dynamic aspect of cyber security—new weakness are constantly being found and defenses are evolving—may best be incorporated into the probability function rather than making production functions dynamic although the latter remains a possibility. Similarly, behavioral models of probability as with cumulative prospect theory may be descriptively appropriate to consider as synthesized by Waaker [18].

4. Conclusion

Previous categories of costs from cyber improvements and losses have conformed to general professional categories but have not been specific about the pathways through which gains and losses can occur. This paper brings information, both internal and external, into the canonical structure of microeconomic models of the consumer, the firm, and government. Impacts are then identified through the full set of partial derivatives for utility, price, quantity, profit, and taxes. The increased definitional detail facilitates the use of statistical tools to study the behavior of consumers and the firm.

Acknowledgements

Appreciation is extended to Anupam Joshi, Matt Shabat and Jules Szanton for comments and discussion. Funding was provided by the Department of Homeland Security National Center on the Risk and Economic Analysis of Terrorism Events (CREATE).

References

[1] Gordon, L. and Loeb, M. (2002) The Economics of Information Security Investment. *ACM Transactions on Information and System Security*, **5**, 438-457. http://dx.doi.org/10.1145/581271.581274

[2] Bikhchandani, S., Hirshleifer, J. and Riley, J.G. (2013) The Analytics of Uncertainty and Information. 2nd Edition, Cambridge University Press, Cambridge. http://dx.doi.org/10.1017/CBO9781139016209

[3] Rogerson, R., Shimer, R. and Wright, R. (2005) Search-Theoretic Models of the Labor Market: A Survey. *Journal of Economic Literature*, 959-988. http://dx.doi.org/10.1257/002205105775362014

[4] Farrow, S. and Szanton, J. (2016) Cybersecurity Investment Guidance: Extensions of the Gordon and Loeb Model. *Journal of Information Security*, **7**, 15-28. http://dx.doi.org/10.4236/jis.2016.72002

[5] Gordon, L., Loeb, M., Lucyshyn, W. and Zhou, L. (2015) Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model. *Journal of Information Security*, **6**, 24-30. http://dx.doi.org/10.4236/jis.2015.61003

[6] Levinson, D. (2002) Encyclopedia of Crime and Punishment. Vol I, Sage Publications.

[7] Anderson, R., Barton, C., Boehme, R., Clayton, R., van Eeten, M., Levi, M., Moore, T. and Savage, S. (2012) Measuring the Cost of Cyber Crime. Workshop in the Economics of Information Security (WEIS).

[8] Undercofer, J., Joshi, A. and Pinkson, J. (2003) Modeling Computer Attacks: An Ontology for Intrusion Detection. *Proceedings of the Sixth International Symposium on Recent Advances in Intrusion Detection*. http://dx.doi.org/10.1007/978-3-540-45248-5_7

[9] Detica and the Office of Cyber Security and Information Assurance (2011) The Cost of Cybercrime, February. https://www.gov.uk/government/publications/the-cost-of-cyber-crime-joint-government-and-industry-report

[10] Becker, G. (1965) A Theory of the Allocation of Time. *Economic Journal*, **75**, 493-517. http://dx.doi.org/10.2307/2228949

[11] Gronau, R. and Hammermesh, D. (2006) Time vs. Goods: The Value of Measuring Household Production Technologies. *Review of Income and Wealth*, **52**, 1-16. http://dx.doi.org/10.1111/j.1475-4991.2006.00173.x

[12] Campbell, K., Gordon, L.A., Loeb, M. and Zhou, L. (2003) The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market. *Journal of Computer Security*, **11**, 431-448. http://dx.doi.org/10.3233/JCS-2003-11308

[13] Eeckhoudt, L., Gollier, C. and Schlesinger, H. (2005) Economic and Financial Decisions Under Risk. Princeton University Press, Princeton.

[14] Clemen, R.T. and Reilley, T. (2001) Making Hard Decisions. Duxbury Press, Belmont.

[15] Keeney, R.L. and Raiffa, H. (1976) Decision Making with Multiple Objectives Preferences and Value Tradeoffs. Wiley, New York.

[16] Della Vigna, S. (2009) Psychology and Economics: Evidence from the Field. *Journal of Economic Literature*, **47**, 315-372. http://dx.doi.org/10.1257/jel.47.2.315

[17] Farrow, S. and Scott, M. (2013) Comparing Multi-State Expected Damages, Option Price and Cumulative Prospect Measures for Valuing Flood Protection. *Water Resources Research*, **49**, 2638-2648. http://dx.doi.org/10.1002/wrcr.20217

[18] Wakker, P. (2010) Prospect Theory for Risk and Ambiguity. Cambridge University Press, Cambridge. http://dx.doi.org/10.1017/CBO9780511779329