SAND2013-2305C

Timeframe for investing in cyber security does matter: A brand value argument

Munaf S. Aamir*, Walter E. Beyeler, Andjelka Kelic, Michael Mitchell,
Sandia National Laboratories[1], Albuquerque, New Mexico, USA
{msaamir, micmitc, webeyel, akelic}@sandia.gov

Abstract. U.S. Presidential Policy Directive (PPD) 21 emphasizes the need for improvement of cyber security throughout the critical infrastructure enterprise. The majority of published studies on the economics of cyber security focus heavily on the development of optimal investment strategies in cyber security. However, national cyber security policy requires the consideration of value beyond what is perceived at a single firm. This conference paper recommends the addition of model structure to Dutta and Roy's published SD work on modeling cyber security investment policy. We propose and implement model structure that resolves a basic assertion in the Dutta and Roy model that states "that a delay in implementation of cyber security has no statistically significant impact on business value realized." We pose that if a cyber security lapse is serious enough, there may not be a business left to deliver value. We do this by including theories on brand value and consumer confidence in our dynamic hypothesis and model.

Keywords: Cyber Security, Brand Value, Consumer Confidence

1. INTRODUCTION

U.S. Presidential Policy Directive (PPD) 21 emphasizes the need for improvement of cyber security throughout the critical infrastructure enterprise. PPD 21 will survey the cyber security protection throughout critical infrastructure and provide minimal standards for ensuring cyber security. The intent these standard is to highlight the value of the service provided by critical infrastructure to the nation, and to consider that value when investing in cyber security.[9]

The majority of published studies on the economics of cyber security focus heavily on the development of optimal investment strategies in cyber security. These studies perceive cyber security as a technological problem in which firms can decide to adopt a technology based on the perceived marginal cost and benefit irrespective of the interplay of human interaction and behavior.[10] Investment strategies proposed in these studies may help individual firms, but are not practical for establishing national-level cyber security policies.

National cyber security policy requires the consideration of value beyond what is perceived at a single firm. To date, only handful of studies in the published literature account for behavioral considerations of cyber security. The most notable in system dynamics is a 2008 study by Dutta

[1] Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

and Roy, in which a system dynamics model is constructed to include the value that good cyber security has on business.[10]

Understanding the business value of cyber systems is important and Dutta and Roy provide a good initial structure for analyzing policy. However, Dutta and Roy miss a key issue when considering the timing of the cyber security investment. In their conclusions, Dutta and Roy stated "that the delay in implementing infosec investments did not have a statistically significant impact on the business value realized."[10] Evidence (although sparse) and corporate disclosure policy suggests that this assertion does not reflect observed behavior under cyber security breaches. [4] [11]

In this conference paper we propose an addition to the Dutta and Roy model to consider how clients of the company impacted by cyber-crime can increase long-term costs stemming from a cyber attack on a company.

1.1. Brand Value

In finance, brand value is used to quantify the total value of a company that includes income, future income, reputation, and market value. Companies estimate how much cyber-attacks will impact brand value when determining investment in cyber security infrastructure [7]. In addition, companies are fearful of disclosing any information of cyber attacks on the fear that it could negatively affect their brand value. News reporting has uncovered that many companies a are unwilling to disclose attack information because they fear it can negatively impact reputation and future income through regulatory costs. [11]

1.2. Cyber Security Costs

There are many ways to exploit cyber systems: Distributed Denial of Service (DDoS) attacks [2], data breaches (hacking) [4], and social engineering (phishing) [5]. Whatever the cause of the cyber-attack, the effect is a loss to the institution of data, money, functionality, and/or reputation. Cyber-attacks in the financial industry are common and the effect on customers varies from the inconvenience of disputing a credit card charge to incurring financial loss. A cyber-attack has both direct and indirect costs. The direct costs can be associated with the attack such as the fraud liability, recovery costs, and revenue losses related to the attack. The indirect costs are the effects on customer loyalty and the reputation of the institution. Over time, frequent cyber-attacks, even small ones, can erode customer confidence in the financial institution. Losses in confidence are cumulative and will eventually reach a point where customer might leave. However, companies can regain confidence after a cyber attack given enough time between attacks.

For example, in finance, the exposure to a customer due to a cyber-attack depends more on the type of account compromised than the type of attack. Fraudulent purchases using credit cards have the least financial exposure to customers. When a fraudulent purchase is made using a credit card number (no card-present), the customer is not liable for the fraudulent charge. In the case of a credit card being stolen and used fraudulently (card-present), the customer is not liable for any charge if the card was reported stolen and the customer is only liable for $50 if the card was not reported stolen before the card was used fraudulently [6]. ATM and debit cards afford considerably less customer protection than credit cards. When a fraudulent purchase is made

using the debit card number (no card present) the same rules apply as a credit card, there is no financial liability to the customer. When fraud is purported using a stolen ATM or debit card (card-present), the financial exposure to a customer increases. A customer has two days to report an ATM or debit card stolen before becoming liable for up to $500 of fraudulent charges [6]. A customer has two days to report an unauthorized transfer from the customer's bank account or the customer becomes liable for up to $500. If a customer does not report a fraudulent transfer until after 60 days from the bank statement reporting the transfer, the customer is wholly liable for the loss [6].

1.3. Customer Behavior and Potential Loss of Confidence.

Operational considerations are often cited as a major driver for investing in cyber security.[10] However, customers (and investors) can easily become motivators for companies to invest in cyber. This is exemplified by a 2008 incident where the largest Korean internet shopping site was compromised by a hacker resulting in the customer database being stolen; the database contained customer financial information as well as personally identifiable information [4]. MinJae Lee and JinKyu Lee conducted a study on the responses of customers to the hacking incident. The results of the study show a significant number of customers ended their relationship with the online shopping site due to the hacking incident [4]. The negative customer response to the attack was not limited to the customers who had data compromised; customers who did not have their data compromised also cancelled their accounts with the shopping site [4].

Additionally, it is important to assess a potential loss of confidence in a company that is a key component in brand value. Both the response of system users and of operators are potentially important. Useful literature includes the extensive literature of how people develop and lose trust in technological systems and investigations of people's reactions to natural disasters. [13] [14] [15] [16] A preliminary review of these studies suggest that:

- Whether people construe failure as a betrayal of trust dictates reactions to failures of trusted parties (other people, institutions, or technologies). If people see the failure as out of the control of the counterparty, trust is more readily restored [12].
- Actual panic is a rare and unlikely reaction to disruptive events. An event framed as a panic situation produces reactions focused on escaping the threat and on individual survival, which are very rational responses. From this standpoint, generalization from failures of particular systems to similar systems may be unlikely unless there is uncertainty around the integrity of the related systems or unless there is evidence of immediate danger to those systems [16].
- The tendency for fearful reaction depends on the contextual background of the event. The general atmosphere of trust or suspicion in institutions, the existence of strong social ties, and uncertainties about the nature of the threat and social roles all play a role in how likely generalization is to occur ([16]).

2. MODEL DEVELOPMENT

We built an SD model to analyze the change in brand value due to multiple cyber-attacks. Figure 1 is a causal loop diagram (CLD) elucidating the core logic of our model. Our model contains three feedback loops: two positive reinforcement loops (R1, & R2) and a balancing loop (B1). This diagram illustrates the casual relationships between stocks and flows. Positive (+) relationships between variables represent proportional movements in those variables, whereas negative (-) relationships represent inversely proportional movements between variables. We focus on the reinforcement loop to study how customer loyalty effects brand value.

2.1. Causal Loop Diagram

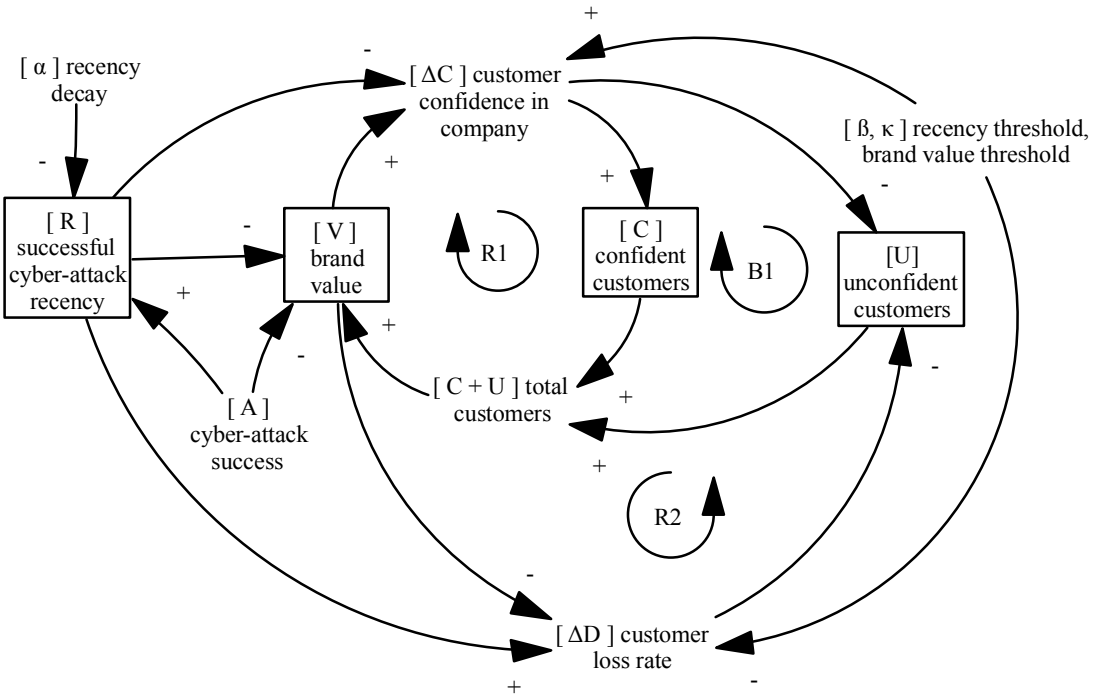

Fig. 1. Causal Loop Diagram of Model

Loop R1 describes the impact brand value has on customer confidence. A high brand value provides friction to loss of confidence after a cyber-attack; conversely a low brand value will cause more customers to become unconfident or depart after an attack. As customers leave, brand value degrades yielding further decline in customer confidence. When memory of the attack wants, unconfident customers can regain confidence.

Loop B1 describes how customers become unconfident after recent cyber-attacks. The memory of recent cyber-attacks accumulates causing an erosion of consumer confidence. A lower level of consumer confidence causes more customers to move from the confident to unconfident, and eventually leave the institution. This degrades brand value decreasing confidence
Loop R2 describes the impact brand value has on customer departure. As brand value decreases, more customers wish to leave the institution. This reduction in customers causes a decline in brand value. This process is remediated as the memory of recent cyber-attacks wanes.

2.2. Model Formulation

A cyber-attack has a direct impact on an institution's customer-base. The indirect impact of a cyber-attack is measured by a change in customer confidence. The recency of a cyber-attack causes customers to lose confidence in an institution. We model recency (R) as:

$$\frac{dR}{dt} = A - R\alpha\,, \tag{1}$$

where, A is a signal of new successful attacks, and α is the recency decay rate. We model the impact caused by the recency of a cyber-attack to customers in the following equation:

$$E = \left(\frac{R}{\beta} - 1\right)^3 + 1\,, \tag{2}$$

where β is the recency threshold. This equation characterizes the small number (less than β) attack phenomenon where customers will react with marginally increasing concerns. These concerns will inflect when attach recency equals β. If recency of attacks becomes greater than β, customers will leave the institution at increasingly higher rates.

Customer confidence ultimately drives the number of customers an institution services. The model has two state variables which track customer populations: confident customers (C) and unconfident customers (U). Customers must first become unconfident before deciding to leave the institution. If a major loss in confidence within the institution occurs, the institution could survive as long as their brand value does not decrease significantly. In the model we define the flow of customers from confident to unconfident as follows:

$$\Delta C = -C\gamma BE + U\delta\,, \tag{3}$$

where B is brand value effect as defined by the equation $e^{-V/\kappa}e$ which estimates the impact of brand value (V), γ is the loss of confidence fraction, and δ is the regaining confidence fraction. The loss of customer confidence is defined by the term $-C\gamma BE$. The effect of brand value provides friction to loss of customer confidence as long as V remains greater than κ (brand value threshold). A smaller κ value will result in a smaller change in customer confidence due to cyber-attacks.

Unconfident customers will flow back to confident customers as defined by $U\delta$ where the greater δ, the faster people will regain confidence in the institution. We assume B does not impact return to confidence. Customers leave the institution when their confidence in the institution is low and the brand value of the institution is also low. We model this as follows:

$$\Delta D = U\varepsilon BE\,, \tag{4}$$

where D is the departure rate and ε is the departure fraction.

Brand value (V) is defined as follows:

$$\frac{dV}{dt} = -V\left(\frac{dX}{dt}\zeta - A\eta\right) + \left(\frac{\theta - V}{\vartheta}\right), \quad (5)$$

where $\frac{dX}{dt}$ is the trend in number of total customers as defined by $\frac{dX}{dt} = \left(\frac{C+U-X}{\iota}\right)$, ζ is the customer outlook multiplier, η is the brand value loss fraction from attack, θ is the max brand value, and ϑ is the time to rebuild brand value. V, is negatively affected by loss of customers and cyber-attacks. The term $\frac{dX}{dt}$ models customer trend. The function accomplishes this by averaging the current number of customers with a previous measure of the trend over a given time (ι). Cyber-attacks (A) proportionately impact V. As the information of a cyber-attack is made public, components of brand value such as shareholder equity and reputation are impacted. The model assumes an exponential recovery of V to value θ, over a given period of time, ϑ.

3. ANALYSIS

We studied the sensitivity of a customer behavior parameter in environments of disparate periodicity of cyber-attacks and the effects on brand value. First we configured a baseline simulation, based on the current literature, to tuned our model to show how we expect customers to react to an infrequent periodicity of cyber-attacks. Second we performed a sensitivity analysis by sweeping over various parameters and environments subject to increasing frequencies of cyber-attack.

3.1. Baseline Simulation

We configured a simulation where customers and were subjected to a cyber-attack once a year. The simulation lasted for 37 months and the customers' recency decay rate was 0.5, signifying a customer's memory of past cyber-attacks decays by 50% each month since the incident. This simulation is our base case and represents the nominal behavior expected after a single cyber-attack.

Figure 2 illustrates the trajectory of brand value in a simulation where a cyber-attack occurs annually, beginning in month two. Initially brand value starts at 100. Brand value drops immediately after the first cyber-attack. Brand value begins to recover before it dips again. This is caused by the latency between cyber-attack and customer departure. The latency effect is a result of the customer's memory of the cyber-attack and the time that it takes for customers to become unconfident and decide to depart the institution. Over time brand value recovers until the company is subjected to another cyber-attack. Brand value is minimally impacted as the result of an annual cyber-attack and is almost fully recovered by the time the next cyber-attack occurs. The recovery of brand value is due to the customers' recency decay rate. The baseline decay rate allows customers to forget a single cyber-attack within a year, thereby decreasing the number of unconfident customers and the negative impact to brand value. This kind of model behavior is what a complete cyber investment model should consider.

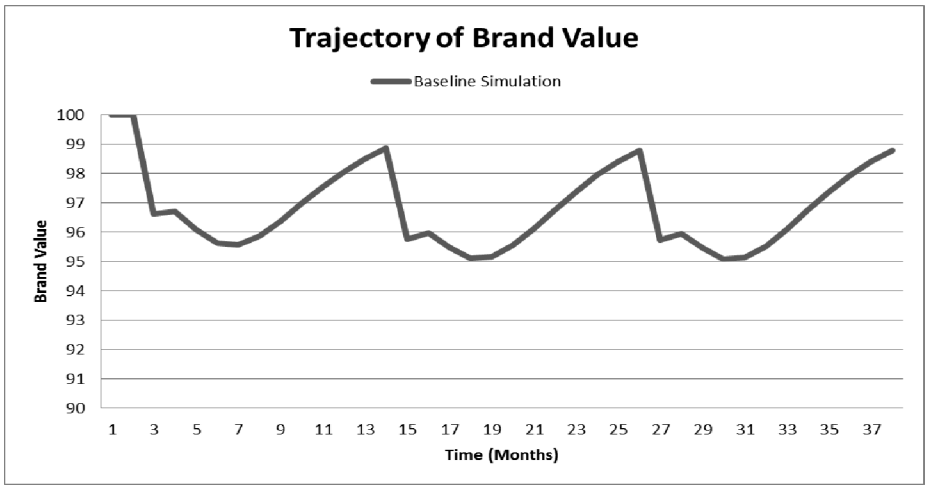

Fig. 2. Trajectory of Brand Value over Time for the Baseline Simulation

3.2. Sensitivity Analysis

We conducted a sensitivity analysis to study how the variation in the departure fraction affects brand value in environments of disparate periodicity of cyber-attacks. For each simulation run, we reported the minimum point of the brand value curve. Each simulation modeled one institution with one million customers and the simulation was run for 37 months. We modeled cyber-attack intervals on a yearly, biannually, quarterly, bimonthly, and monthly basis. We selected three departure fraction values to study: 0.1, 0.2, and 0.3 where 0.1 represented the least amount of customers departing post-cyber attack, and 0.3 represented the largest percentage of customer defecting.

Figure 3 expresses the results of the sensitivity analysis. The results of the study indicate that as the frequency of attacks increase, the negative impact to brand value is non-linear. When the frequency of attacks increases from biannual to quarterly, brand value is significantly impacted. This non-linearity is hard to predict. The reason for why firms lose brand value is ultimately tied to the loss of customer confidence.

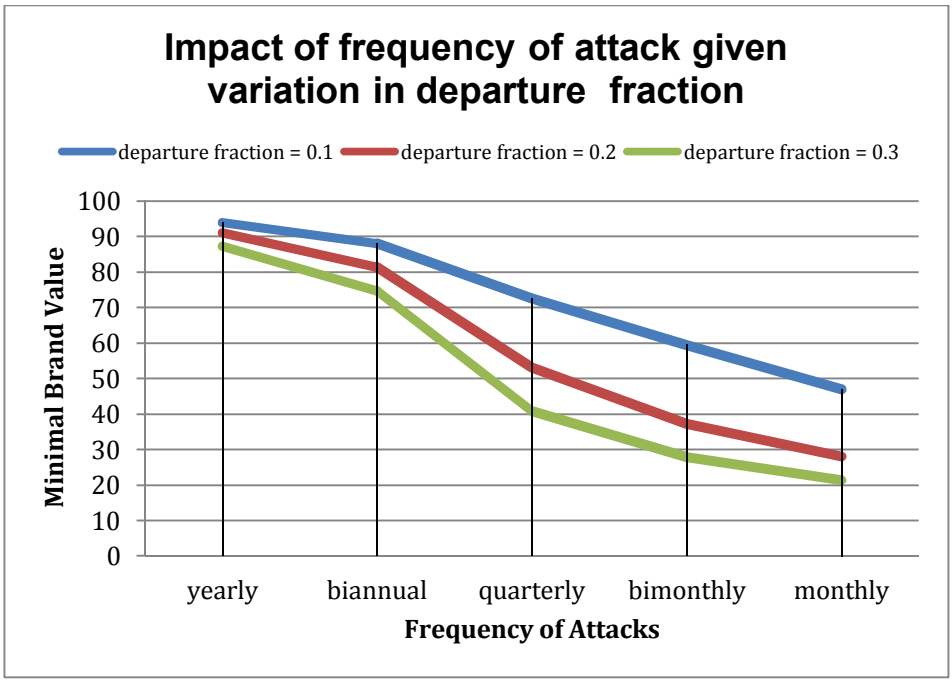

Fig. 3. Impact of frequency of attack given variation given different departure fractions (how sensitive consumers are to departing given cyber attacks. Note: Departure of customer reinforces the loss in brand value.

Additional parameter analyses were completed and are presented below:

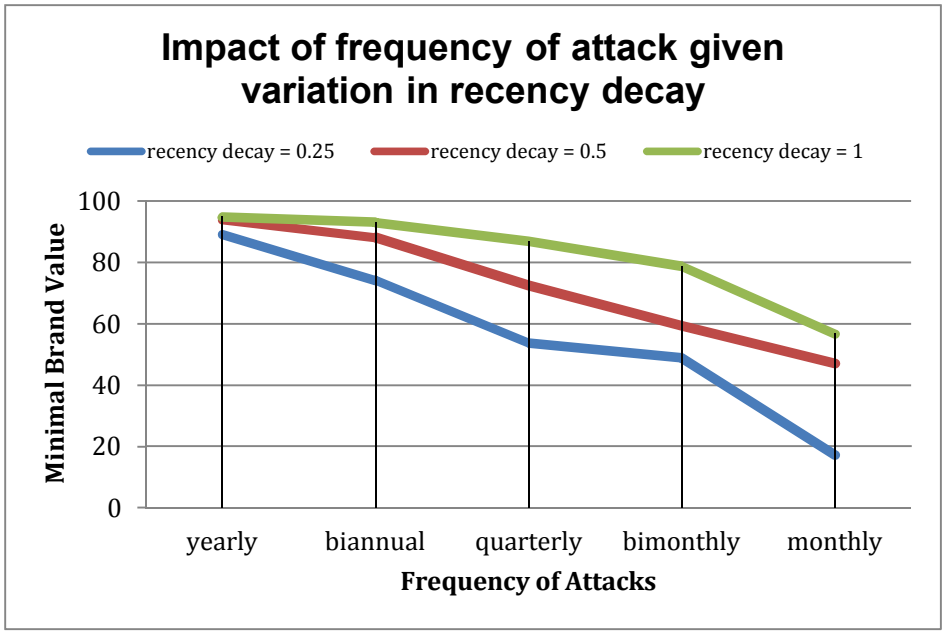

Fig. 4. Impact of frequency of attack given the variation in recency decay value. Note: recency decay is the fraction at which customer memory of the attack decays.

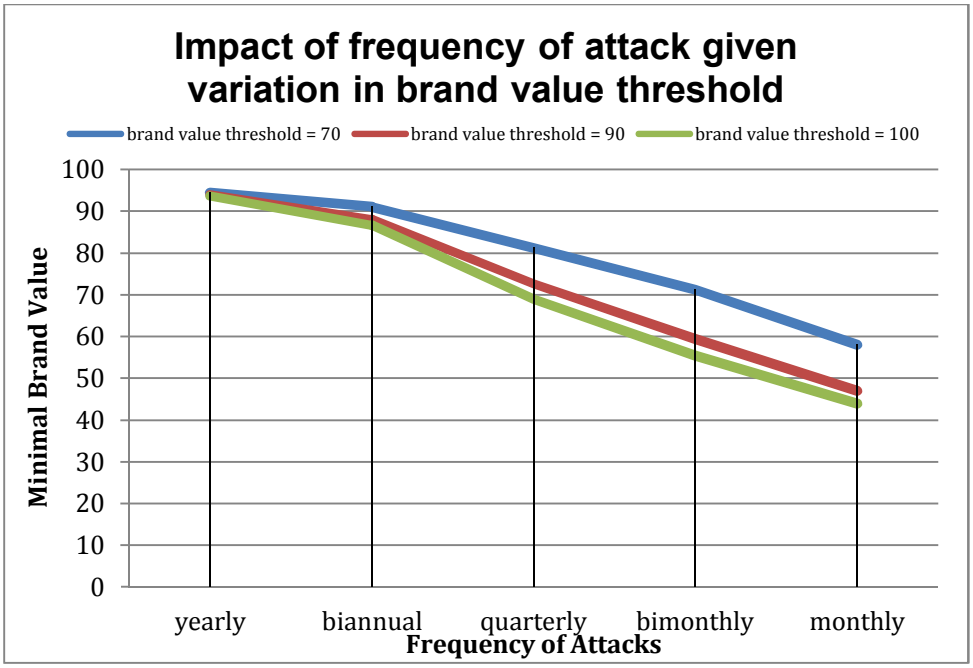

Fig. 5. Impact of frequency of attack given variation in brand value threshold. Note: Brand value threshold is a value that controls the rate at which people perceive that a brand is "bad."

4. CONCLUSION & FUTURE RESEARCH

Investment in cyber-security needs to include an estimation of the impact to brand value from multiple cyber-attacks. Infrequent cyber-attacks have a predictable impact to brand value. As the frequency of cyber-attacks increase, the effect on brand value becomes non-linear and more difficult to predict. Consumer behavior is the most important factor in estimating the impact to brand value from a cyber-attack.

We recommend improvements in the estimation of customer confidence. This will provide a better characterization of how to invest in cyber-security. With each successful cyber-attack, a fraction of customers become unconfident and a fraction of the unconfident customers will leave. If the unconfident customers have not had the opportunity to recover their confidence when subsequent attacks occur, more customers will become unconfident and more of them will leave. Developing improved characterization techniques for both the effect of frequency of attacks and confident versus unconfident customers would greatly improve national cyber-investment strategy, thereby protecting brand value.

This paper describes a dynamic hypothesis and pursues a simple model to explain the overall hypothesis. Next steps in our research will involve integrating these dynamics into the model developed by Dutta and Roy. The biggest problem in researching response to cyber attacks is the lack of published data. In our future research we will attempt to model a real case such as the one described by Lee, MinJae and Lee, JinkKyu. This will help to better assess the true customer impacts of cyber attacks.

References

1. Anderson, Ross: Why Information Security is Hard - An Economic Perspective. Annual Computer Security Applications Conference. 2001.
2. CERT: Results of the Distributed-Systems. Intruder Tools Workshop, Software Engineering Institute, Carnegie Mellon University. December 7, 1999
3. RM Brady, RJ Anderson, RC Ball: Murphy's law, the fitness of evolving species, and the limits of software reliability. Cambridge University Computer Laboratory Technical Report no. 476. 1999;
4. Lee, MinJae and Lee, JinKyu: The impact of information security failure on customer behaviors: A study on a large-scale hacking incident on the internet. Information Systems Frontiers. Volume 14, Number 2 (2012), 375-393, DOI: 10.1007/s10796-010-9253-1.
5. Gisin, M. Phishing: Kriminalistik v:62 i:3 p:197-200. 2008. issn:00234699.
6. FTC. www.ftc.gov/bcp/edu/pubs/customer/credit/cre04.shtm. 10/31/12.
7. Dynes, S., Goetz, E., and Freeman, M. Cyber Security: Are Economics Incentives Enough? IFIP International Federation for Information Processing, Volume 253, Critical Infrastructure Protection, eds. E. Goetz and S. Shenoi; 2008, (Boston: Springer), pp. 15–27.
8. Ajzen, Icek. Theory of Planned Behavior. Organizational Behavior and Human Decision Processes 50, 179-211 (1991).
9. The White House. Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience. 2013.
10. Dutta, Amitava, Roy Rahul. Dynamics of organization information security. *System Dynamics Review*. pp. 349-375. Cambridge, MA. Volume 24. 2008.
11. Javers, Earmon. Cyberattacks: Why companies keep quiet. CNBC 2013.
12. Bisantz, A.M. and Y. Seong, "Assessment of operator trust in and utilization of automated decision-aids under different framing conditions," International Journal of Industrial Ergonomics, 28, 85-97: 2001.
13. Koehler, J.J., and A.D. Gershoff, "Betrayal aversion: When agents of protection become agents of harm," Organizational Behavior and Human Decision Processes, 90, 244-261: 2003.
14. Lewandowsky, S., M. Mundy, and G.P.A. Tan, "The dynamics of trust: Comparing humans to automation," Journal of Experimental Psychology: Applied, 6, 104-123 2000.
15. Parasuraman, R., and V. Riley," Humans and automation: Use, misuse, disuse, abuse," Human Factors, 39, 230-253: 1997.
16. Quarantelli, E.L., "Panic behavior: Some empirical observations," presented at the American Institute of Architects Conference on Human Response to Tall Buildings, July 19, 1975, Chicago, Illinois: 1975.