

Macro-Economic Cyber Security Models

Matt Kiely, Eric Kobe, Amanda MacArthur, Matt Polk, Eric Rains,
Eva Andrijcic, Jonathan Crawford, and Barry Horowitz

Abstract—This paper quantitatively addresses two issues concerning cyber security economics that prior efforts have not. The first involves cyber security and its effect on a company’s reputation. In this case, we focus on the levels of investment companies make related to reputation and how they implicitly reveal their views on cyber security risks. The second involves cyber security regulations. This analysis compares different strategies for choosing companies to regulate and the corresponding levels of risk reduction. This analysis can be used by companies and government policy makers to address cyber security investments decisions.

A company’s reputation is fundamental to their economic future. An advertisement, or article containing a security breach, can effect their reputation. This paper assumes the rate of advertising is indicative of the value they place on their reputation; hence, this is related to the value they place on cyber security. Comparing spending practices will provide insight into the value a company places on cyber security in regard to preserving their reputation. Early results show some difference in spending among banks, as well as sharper differences between banks and retail sectors in evaluating cyber security. In addition, an expected consequence analysis is performed to compare alternative investment strategies for cyber security components focused on reputation, as measured by the likelihood of a possible cyber attack resulting in media coverage. Historical data provides the basis for results that reveal the consequences implicitly being avoided by companies as a function of their level of investment and other economic variables.

The second part of our analysis involves the macroeconomic effects of cyber attacks and their relationship to government regulations. Since cyber attacks have the potential for large indirect economic effects, the need for regulation is apparent. Although cyber security regulations requiring reporting of events currently exist, most security measures are the result of private industry decision-making rather than government

influence. This analysis will determine the firms that provide the most economic influence from a risk reduction viewpoint. This analysis explores alternative methods to select firms for possible regulation and compares the level of risk reduction for these choices by using input-output modeling.

I. INTRODUCTION

THIS project involves assessing the economic consequences of cyber attacks and cyber security investments. Cyber attacks include viruses, worms, trojan horses, phishing, denial of service attacks, unauthorized access and control system attacks [1]. Regardless of the type or severity, a cyber attack can cost corporations a substantial amount of money in goods, reputation, and time [2]. Individuals are also vulnerable. Excluding the potential implicit losses, The Gartner Group, an information technology research and advisory company, reported “between May 2004 and May 2005, roughly 1.2 million U.S. computer users suffered phishing losses valued at \$929 million” [3]. Therefore, the protection of digitized information is equally as important as that of physical assets [4]. As computers become more integrated into modern life, the importance of information security continues to rise. The frequency of cyber attacks is also increasing, and the severity of future attacks could be much greater than what has already been observed [5].

In this paper risk analysis is being conducted at both the macro-economic level, involving sectors of the US economy, and the micro-economic level related to individual firms. The three main aspects of cyber security that were explored are: 1) the relationship between a company’s reputation and their cyber security concerns, 2) strategies for regulation and standardizations, and 3) the significant role that several small private companies play in determining the level of cyber security for the Internet.

II. REPUTATION

A. Framework

This section presents three models that isolate cyber security investments intended to protect reputation. Company financial data are used to estimate model parameters and calculate model outputs for companies in the banking, credit, and retail sectors. The model outputs illustrate current company perceptions of the coupling between cyber risk and reputation risk. These outputs show that trust-oriented companies perceive that cyber attacks are a significant threat to reputation. The models create a

Manuscript received April 14, 2006. This work was supported in part under Award number 2003-TK-TX-0003 from the U.S. Department of Homeland Security, Science and Technology Directorate. Points of view in this paper are those of the author(s) and do not necessarily represent the official position of the U.S. Department of Homeland Security or the Science and Technology Directorate. The I3P is managed by Dartmouth College.

M. Kiely (e-mail: mnk9f@virginia.edu), E. Kobe (e-mail: ek4t@virginia.edu), A. MacArthur (e-mail: asm2k@virginia.edu), M. Polk (e-mail: mwp2x@virginia.edu) and E. Rains (e-mail: er7f@virginia.edu) are students in the Department of Systems & Information Engineering at the University of Virginia, Charlottesville, VA 22904 USA.

E. Andrijcic (e-mail: ea2r@virginia.edu) and J. Crawford, (e-mail: jac2bp@Virginia.edu) are graduate research assistants in Systems & Information Engineering at the University of Virginia, Charlottesville, VA 22904 USA.

B. Horowitz (e-mail: bh8e@virginia.edu) is a Professor of Systems & Information Engineering at the University of Virginia, Charlottesville, VA 22904 USA.

framework companies can use to analyze their cyber security investment decisions.

B. Data

Company data were collected from various sources. Advertising spending data from 2004 was obtained from Advertising Age [6], which collects and sells advertising news. In addition, Yahoo Finance supplied the means to collect revenue, net income, profit margin, and other financial information for each company [7].

Cyber security investments were approximated using data from Forrester Research, which identifies and analyzes trends in technology. First, the research team obtained 2004 IT spending forecasts as percentages of company revenue according to industry. It was then estimated that three percent of IT spending is invested in cyber security for all companies studied [8]. Using these estimates, cyber security spending was approximated as a function of company revenue and the industry in which the company resides (e.g., banking, retail).

The next step in the study involved calculating the probability of a publicly announced security breach for companies with more than 5,000 employees. Accomplishing this required counting the number of security breaches for companies with more than 5,000 employees from February 15th, 2005 to February 15th, 2006 [9]. The total number of companies in the U.S. with over 5,000 employees was then collected from the U.S. Census Bureau [10]. Assuming that all companies are equally at risk, calculating the probability of an attack on an individual company over the course of a year simply required dividing the number of companies that had a security breach by the total number of 5000 or more employees U.S. companies. In addition, the probability of an attack was separately calculated for the finance (banking and credit cards) sector and the retail sector. Using this data, three models were developed.

C. Reputation Model

The reputation model illustrates the minimal amount of revenue a company implicitly expects to lose from a publicized security breach based on the percentage of their cyber security budget allocated for reputation. While it is recognized that companies do not explicitly allocate a budget related to their reputation, companies do view reputation as an important reason for investing in cyber security solutions. The models presented here make the reputation reason economically explicit. The variables used for this model and the two models that follow are summarized below:

β = Probability of Publicized Security Breach without Additional Investment Focused on Reputation

α = Probability of Publicized Security Breach after Additional Investment Focused on Reputation

P = Profit at Risk from a Publicized Security Breach

V = Revenue at Risk from a Publicized Security Breach

PM = Profit Margin

C = Cost of Cyber Security Spent for Reputation

M = Return on Investment Multiplier for Advertising Investments

MC = Reduction in Market Cap Expected due to a Publicized Security Breach

RM = Market Cap to Revenue Ratio

In addition, there are a number of assumptions used for this model and the two subsequent models. The list of assumptions are as follows:

Cyber security costs represent money that could be invested in other opportunities for the company, such as advertising.

β is the current observed probability of a successful attack.

The added, reputation focused, cyber security investment, C, is made in the hope that no publicized security breaches will occur, or that the probability of a publicized cyber attacked will be reduced to nearly zero. ($\alpha = 0$).

The following mathematical steps are used to achieve equation 1.0.

$$\beta * P \geq C + \alpha * P$$

$$\beta * P - \alpha * P \geq C$$

$$(\beta - \alpha) * P \geq C$$

$$(\beta - \alpha) * \frac{P}{PM} \geq \frac{C}{PM}$$

$$(\beta - \alpha) * V \geq \frac{C}{PM} \quad (1.0)$$

Setting α to 0 and solving for V yields equation 2.0,

$$V \geq \frac{C}{PM * \beta} \quad (2.0)$$

Equation 2.0 shows that companies should not be expected to spend more on reputation related security than the expected amount of profit they would lose due to a publicized security breach.

D. Expanding the Model to Opportunity Cost

Cyber security investments represent money that could be spent in other areas of the company, such as advertising. The amount of revenue generated from advertising is expected to exceed the amount of the advertising investment. As a result, the opportunity cost for spending money on cyber security would be higher than equation 2.0 would indicate.

Using the following mathematical steps, equation 3.0 is obtained.

$$\beta * P \geq C * M + \alpha * P$$

$$\beta * P - \alpha * P \geq C * M$$

$$(\beta - \alpha) * P \geq C * M$$

$$(\beta - \alpha) * \frac{P}{PM} \geq \frac{C * M}{PM}$$

Setting α to 0 and solving for V yields equation 4.0,

$$V \geq \frac{C * M}{PM * \beta} \quad (4.0)$$

In equation 4.0, the opportunity cost related to investments in cyber security is taken into consideration. V represents the minimal amount of revenue that a company expects to lose from a security breach. The cost of cyber security spent on regulation, C , is multiplied by the opportunity cost multiplier, M , since the opportunity to use the investment on advertising is lost.

E. Expanding the Model to Market Capitalization

An information security breach that affects company revenue would ultimately affect the market cap. This model shows the least amount of market cap a company can expect to lose from a security breach.

The following mathematical steps show how equation 5.0 was computed,

$$\begin{aligned} \beta * P &\geq C * M + \alpha * P \\ \beta * P - \alpha * P &\geq C * M \\ (\beta - \alpha) * P &\geq C * M \\ (\beta - \alpha) * \frac{P}{PM} &\geq \frac{C * M}{PM} \\ (\beta - \alpha) * V &\geq \frac{C * M}{PM} \\ (\beta - \alpha) * V * RM &\geq \frac{C * M}{PM} * RM \\ (\beta - \alpha) * MC &\geq \frac{C * M}{PM} * RM \quad (5.0) \end{aligned}$$

Setting α to zero and solving for MC yields equation 6.0,

$$MC \geq \frac{C * M * RM}{PM * \beta} \quad (6.0)$$

Equation 5.0 and 6.0 show that market cap, MC , can be calculated to show the minimum amount of market cap a company expects to lose from a security breach.

F. Results

These models provided insight into each company's perception of the potential reputation-related consequences of a security breach. The potential loss of revenue, opportunity cost from not investing in advertising, and potential market cap loss were all analyzed for each company, and the sectors were compared. The differences in the results among sectors can be attributed to two main variables. First, beta for the finance industry (banking and credit cards) was 2.8%, while the retail industry had a beta of 0.7%. This means that the banking industry had four times the number of publicly announced security breaches as the retail sector. Second, the profit margins for the finance industry were higher overall than the retail industry. Due to these facts, unifying behavior existed for each industry in the models. Companies within each industry tended to cluster together. However, differences did exist among the different sectors.

The reputation graph in the appendix, Fig. 4, shows that reputation is most important to the banking industry. By fixing the implied percent loss of revenue from a security breach at 25%, the sectors could be compared. According to our reputation model, companies in the banking industry

should be willing to spend the most for cyber security related to reputation. On average, banks would spend 33.5% of their cyber security budgets (their overall cyber security budgets could be estimated from Forrester data on averages for percentage of revenue spent on cyber security per sector) for reputation in order to protect 25% of revenue. Credit card companies should be prepared to spend the most after banks at 21.75%. Retail companies were last, with spending predicted at 11.76%. These results show that banks should be willing to spend three times more than retail for cyber security for reputation. This demonstrates that banks perceive a greater risk of a reputation loss than credit card companies and retailers. However, banks still might not be spending enough, since banks are four times as likely to have reputation impacting attacks.

The opportunity cost graph, Fig. 5 in the appendix, shows that retail companies can expect to give up the most potential revenue by investing in cyber security as compared to investing in advertising. In Fig. 5, the percent of cyber security spent for regulation is fixed at 25%. Fixing the advertising opportunity cost multiplier at 1.50 allowed for the different sectors to be compared. The retail industry, on average, had 97% implied total revenue at risk. The credit card industry followed with 44%. Lastly, banks had 28% implied total revenue at risk. This shows that the retail industry gives up the most opportunity by investing in cyber security as opposed to advertising.

The final analysis performed illustrated that the expected number of years' worth of advertising revenue lost from a publicly announced security breach is highest for the banking industry. By fixing the percent of cyber security budgets allocated to reputation concerns the sectors could be compared. Banks expected to lose, on average, 6.73 years' worth of advertising revenue. This was followed by retailers at 2.02 years, and credit card companies at 1.42 years. Banks expect to lose more years' worth of ad revenue due to the fact that they anticipate losing the most revenue from a reputation attack, and they expect to make the least amount of ad revenue each year. Retail companies, on the other hand, do not suppose losing much revenue from a reputation attack, and they expect to make a lot on ad revenue each year.

The results presented above are based on a number of estimates about individual company investments derived from available integrated data. Not all company data was available to make exact calculations. However, individual companies have the necessary information to derive results pertinent to their businesses more precisely. These models should provide company executives with a useful tool to determine the appropriate amount of cyber security spending.

III. REGULATION

This section quantitatively addresses issues related to cyber-security regulation through economic analysis and

mathematical modeling. The analysis consists of three models: one for assessing cyber-security investments for individual firms, one for helping to determine if government should regulate a given industry and one that considers the percentage of regulation costs that a firm can view as a beneficial investment in cyber-security. The models included data for sixty firms from ten different industries in which cyber-security is important. The data came from four sources, the Bureau of Economic Analysis (BEA), Forrester, Hoover business information database and Resource Insight financial statement database.

Let:

p: Probability of a successful cyber-attack.

D: Anticipated direct losses from a successful cyber-attack. For analysis purposes, the values were estimated as 1% of a firm's gross sales.

I: Anticipated indirect losses from a successful cyber-attack, where indirect losses refer to ripple effects caused by the attacked company and suffered by companies that have economic interactions with the attacked company. The values were estimated using indirect-to-direct losses ratios.

C_A : The additional cyber-security investment that a company believes is required to prevent high economic impact cyber-attacks and reduce p to near zero. The values were estimated as 25% of a firm's normal cyber-security budget.

C_D : Maximum amount that a firm would actually be willing to spend to reduce p to near zero.

C_I : Maximum amount that government is willing to make a firm spend to reduce the likelihood of successful attacks to near zero

A: Audit cost associated with regulation. The values were estimated as 5% of a firm's cyber-security budget.

B: The percentage of regulation costs that a firm can view as a beneficial investment relative to their individual interests in cyber-security, assuming all industries and government have the same belief about p and each firm is regulated.

The first model (7.0) assesses whether firms are under-investing in cyber-security. For this analysis, it is assumed that there exists only one cyber-security technology that costs C_A and can reduce p to approximately zero. If firms act rationally, then they invest C_A if C_D is greater than or equal to C_A . C_D is the product of p and D. The cyber-security investment decisions is

$$C_D > C_A \quad (7.0)$$

where

$$C_D = p * D$$

If equation 7.0 describes the economic values of a specific firm, then it should be expected to invest C_A in the available cyber-security solution.

The second model (8.0) includes the assumptions from the first model (7.0). This model considers the cyber-security investment decision from the societal viewpoint.

This model determines whether or not the government should regulate. The cost of preventing a cyber-attack in the regulatory scenario includes C_A and A. The consequences of a successful cyber-attack are C_I . C_I is the product of p and I. Indirect losses are losses from a successful cyber-attack that occur to firms in other industries which were not cyber-attacked. The losses cascade to other industries due to the interdependent nature of the US economy. This model focused on indirect losses rather than direct losses because it is assumed that government only regulates if a company is making decisions that adversely effects other companies and the economy as a whole. The equation for this model is

$$C_I > C_A + A \quad (8.0)$$

where

$$C_I = p * I$$

If equation 8.0 holds for any firm, then the government should be expected to regulate that firm. Since government regulates industries rather than firms, the analysis focused on industries that might be subject to cyber security related regulation.

The third model (9.0) assesses B for companies in ten industries. B is the percentage of regulation costs that a company would have, using their own internal evaluation model as represented by equation (7.0), voluntarily invested for deriving direct benefits. Thus B is the value of regulation to the company. The mathematical expression is

$$B = \frac{C_D}{C_A + A} \quad (9.0)$$

Each of the variables can be categorized into three groups: variables known by all firms, variables that firms or the government can estimate accurately but are not publicly known, and variables that no one knows. C_A , C_D , C_I , D, I and A can be set for decision-making purposes by either a firm or government but is not general public knowledge. Equations 7.0 and 8.0 can be rewritten to isolate p:

$$p < \frac{C_A}{D} \quad (7.1)$$

$$p < \frac{C_A + A}{I} \quad (8.1)$$

The variable p was isolated in both equations because it is a parameter that is unknown to all parties. Therefore, the team analyzed the effect of changing p on cyber-security investment decisions.

These models provide insight about cyber-security investments from the perspective of both firms and government. Fig. 1 and Fig. 2, shown in the appendix, demonstrate that for small variations in p, the expected investment results vary dramatically. Fig. 3, from the appendix, shows the relationship between the company's perception of the probability of a successful attack, p, and the value the company places in regulation. For instance, if the company believes that there is a minimal chance of an attack then they will receive no benefit from being regulated

and incurring the entire cost $C_A + A$. The horizontal line across Fig. 3 shows where the company's amount C_D is equal to C_A . The graph shows that different sectors require varying perceptions of the probability of a successful attack to see equal benefit from regulation. Thus the government could use this model to determine which sectors would be more adversely affected by regulation.

Indirect-to-direct ratios are the ratio of indirect losses to direct losses from a reduction in demand or supply (caused by a successful cyber-attack) in one industry. Industries with high indirect-to-direct losses ratios, all other things being equal, should give additional consideration to regulation avoidance as part of their cyber-security investment strategy. Across all industries these ratios range from 0.45 to 1.59. That is, for this range, if a dollar is lost directly, depending on the industrial sector suffering that loss, from 45 cents to 1.49 dollars will be lost indirectly.

The six industries with the highest indirect-to-direct losses ratios are as follows:

- Petroleum and Coal Manufacturing 1.59
- Motor Vehicle Manufacturing 1.55
- Pipeline Transportation 1.47
- Textile and Textile Product Mills 1.46
- Food, Beverage and Tobacco Manufacturing 1.41
- Paper Manufacturing 1.33

Our group developed three models that collectively form an initial quantitative framework for making cyber-security investment decisions. Information limitations dictated that this approach was primarily theoretical. However, firms have access to more accurate numerical estimates of key parameters. Thus, firms can use this framework to provide insight into cyber-security investment decisions.

IV. STANDARDIZATION

Over the years, as the internet has become faster, more reliable, and globalized, enabling easier and faster communication between individuals and business around the world, the need for cyber security became more apparent. There have been efforts to prevent cyber crime, but "if trends continue computer attacks will become more numerous, faster, and more sophisticated" [12]. Cyber security standards as well as government regulation are critical to the security of individuals as well as the U.S. infrastructure. Individuals want their information to be safe and not accessed by unauthorized personnel whereas the government does not want an attack against its infrastructure. There is a need for more government regulation as well as government incentives in order to drive private industry and the U.S. government to use security policies that incorporate best practices. One source states, "A growing yet underestimated threat is that of a cyber attack on U.S. critical information infrastructures. Criminals, terrorists, and foreign governments are exploiting the anonymity and global reach of the Internet to attack the U.S. information infrastructure; perform reconnaissance for physical attack; conduct hostile

information operations; steal money, identities, and secrets; and potentially undermine the U.S. economy" [13]. This task is huge because there are numerous computer systems used for many different purposes, and therefore creating standards for regulation incorporates many variables.

The private industry has many standards that deal with security. These standards have been primarily developed by the International Organization of Standardization (ISO) and the British Standards Institute (BSI). The National Institute of Standards and Technology (NIST) has released many special papers that act as standards. Although these NIST standards are primarily focused for government use, they are easily adaptable to private sector use. By implementing these standards companies aim to increase profits by decreasing the amount of cyber security attacks. This also helps companies adhere to best practices policies making it easier for companies to obtain cyber insurance and improve their reputation.

As discussed earlier in this paper, both direct and indirect economic losses must be considered in order for the government to create appropriate cyber security regulation. Cyber Security Industry Alliance (CSIA) says that 93 percent of consumers consider spyware a severe problem, and "71 percent of consumers believe new laws are needed to protect consumer privacy on the Internet" [14]. The U.S. Government has taken a number of initiatives to promote cyber security, but has had limited success because there are no economic incentives and generally the government is using a passive hands-off approach for cyber security regulation [15].

Thus far the government primarily has regulated financial and medical information. The Gramm-Leach Bliley Act (GLBA) and the Sarbanes-Oxley Act of 2002 (SOX) have resulted in the regulation of financial information. SOX has been used in many organizations to fund cyber security expenses, but this is an indirect effect of this act. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) has protected medical information that is individually identifiable from unauthorized access [16]. With respect to protecting the infrastructure the Energy Policy Act (EPA) provided a start for electricity systems, but many other resources must be taken into consideration. Regulation of electronically controlled utilities is very critical such as "electrical transmission grid, oil and natural gas, water, waste water, chemicals, telecommunications, transportation, banking and finance-and many critical processes" [14]. The outcome of an attack to these systems could be horrific. People could lose resources that are necessary to our economy as well as their wellbeing. Attacks on other less critical systems must be considered as well, since they too have the potential to drastically impact society both from a social as well as economic standpoint.

From the perspectives presented in this paper, it would be helpful for the government to develop analytical models for evaluating the potential benefits of added regulation to protect consumers, industry, and the security of the national infrastructure.

V. INTERNET CYBER SECURITY

The Internet has become a major contributor to our nation's economy. As a result, the level of Internet security is important to our economic future. Lincoln Laboratory, a research and development center at the Massachusetts Institute of Technology, is currently part of an industry effort that is pioneering a technique that should protect Internet users from phishing schemes that collect sensitive information from users by counterfeiting legitimate web sites. DNS Security Extensions (DNSsec) serve to validate the source for the requested domain name through encryption and signatures, thereby impeding common phishing attacks [17]. This new technology makes name look-ups more secure and reduces the risk of counterfeit domain names and altered information. The underlying mechanism for DNSsec is based on cryptographic technology that uses digital signatures [18]. These digital signatures will determine if the information returned is from the correct source or if it has been altered in transmission.

The industrial effort on DNSsec could result in either voluntary industrial implementation or the U.S. Government implementing FDIC rules to promote DNSsec [19]. Documents from Lincoln Laboratory indicate that they believe that banks are the logical early implementers of DNSsec, and they would create demand and serve as trailblazers [19].

A. DNS Attacks

In a recent article, Evers states that cyber criminals are now using DNS servers to intensify their assaults and disrupt online commerce [20]. This type of attack is atypical and very dangerous. The traffic from a typical botnet attack is easier to block because the attacking machines are identifiable [20]. However, blocking DNS queries could also result in blocking legitimate users from sending an e-mail or visiting a website [20]. Evers states that this form of attack allows attackers to hide their identities and makes it harder for victims to find the attack's original source.

Furthermore, using DNS also allows the attack to be amplified, increasing the amount of malevolent traffic to the target [20]. According to Vaughn and Evron, a single DNS query could trigger a response that is 73 times larger than the request [20]. Therefore, "relatively small DNS requests can be employed to cause significantly larger replies from a name server to the spoofed IP address" [21].

B. Recommendation

According to Berlind, Paul Mockapetris believes the Domain Name System (DNS) could answer many of the Internet's identity-theft problems [22]. DNS is already in place and every computer on the Internet already uses it [23]. Furthermore, although others collaborated to develop DNS, Mockapetris wrote the protocol [22]. Therefore, he can provide one of the best opinions for securing the DNS.

However, DNSsec is not without its own faults. Critics argue that DNSsec not only has limitations, such as

difficulty in global implementation, but it also generates new problems. Since more information needs to be transmitted between DNS servers and client systems to complete a request, the full implementation of DNSsec could create bandwidth flooding [22]. However, once implemented, improvements can be made to mitigate this.

Even though DNSsec is not perfect, Mockapetris believes that it currently is the best way to thwart identity theft. According to Mockapetris, "DNS has been growing for twenty years, but during that time, no progress has been made on securing it. As a result, the barriers to forging identity are low and the number of transgressions is on the rise" [22]. Mockapetris faults those searching for a perfect solution, meanwhile ignoring an existing good solution that could be the foundation for the future.

Deployment of DNSsec "would raise the barrier to casual identity theft," the most common identity-related offense [22]. But small companies in charge of DNS management view the cost of implementation as too great, and are waiting for the "perfect" solution. We must not wait for the perfect solution and do what is possible now. The perfect solution might even result from the process.

VI. CONCLUSION

The three aspects of this project deal with companies concerned with their reputation, regulations, as well as a myriad of small companies that control cyber security. While we anticipate the models developed will be helpful – we still face many variations of attacks, and there is not a single uniform solution. According to the models, we have drawn the following conclusions:

A. Reputation

There is a unifying behavior within sectors and a differentiated behavior across sectors. According to our results, a company's willingness to spend money on cyber security to protect their reputation directly relates to their sector. In decreasing amounts this is as follows: Banks, Credit Cards, Retail. The use of newspaper articles to identify cyber security incidents can be used to approximate the likelihood of successful attacks across sectors of the economy. From this we concluded that banks are four times more at risk. Therefore, financial industries should be willing to spend more on cyber security to protect reputation. Our models showed that banks are spending three times as much as the retail sector. Numerical model inputs are available to companies for investment consideration.

B. Regulation

Industries with high indirect-to-direct losses ratios should give additional consideration to regulation avoidance as part of their cyber security investment strategy, all other cyber security factors being equal. Industries with the highest ratios are mostly centered on the manufacturing sectors, ratios across all sectors range from 0.45 to 1.59, implying a

3:1 difference in economic propagation effects. Accounting for the direct value the firm would receive from regulation the economic cost of regulation to the firm is relatively small. This assumes that the likelihood of an attack, and the potential consequences that the government uses for its analysis, are the same as the industries use. This analysis framework can be useful for companies because they will have more information to accurately estimate key parameters that our models require as input.

C. Internet Cyber Security

Users must be warned about common cyber attack techniques, and cyber attacks must be thwarted before they occur. A Phishing attack is an example that illuminates this point. DNS Security Extensions can address phishing by validating the source for the requested domain name through encryption and signatures. Shifting security responsibilities from the end user to the Domain Name System may prevent more attacks.

Even though DNSsec may be the best solution, it is impossible to say how successful it will be, because it is not yet widely deployed [23]. However, future researchers could analyze the costs, logistics, and length of time until full DNSsec implementation in Sweden in order to judge its effectiveness. Following this recommendation, if DNSsec proves to promote greater security then implementation should be smoother.

In general, it is obvious that managing cyber security risks is complex and requires predictions about future attacks. Models that support decision making can be a useful tool for clarifying the role that assumptions play in decisions, and can help companies to determine what assumptions they need to make and record for future analyses what values they choose for their assumptions.

APPENDIX

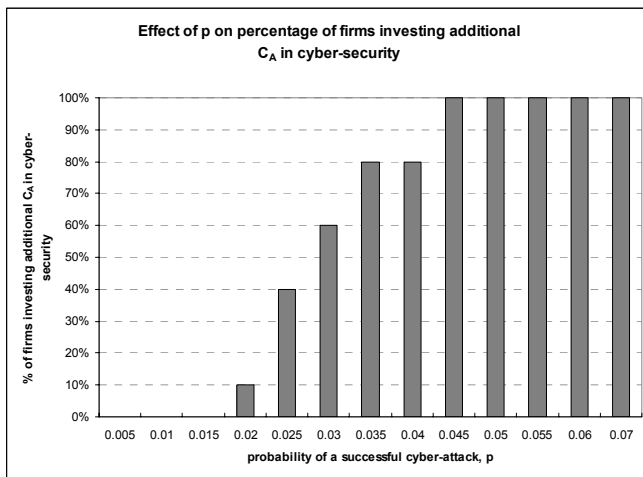


Fig. 1. This shows that for values of p between 0.005 and 0.045, the results vary dramatically changing from 0% of firms investing to 100% of firms investing. For all values of p greater than 0.045, 100% of firms invest.

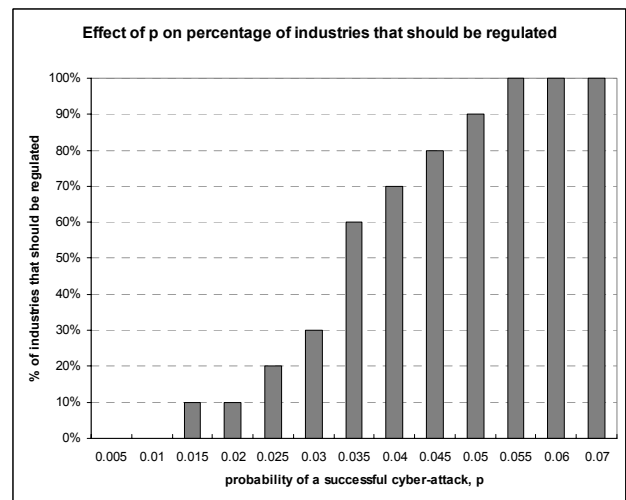


Fig. 2. This shows that for values of p between 0.005 and 0.055, the result varies dramatically changing from 0% of industries regulated to 100%. For all values of p greater than 0.055, 100% of industries are regulated. The first two models show that p has a large effect on the results. Therefore, the value of reducing uncertainty about p is high because the magnitude of losses and cyber-security investment are large.

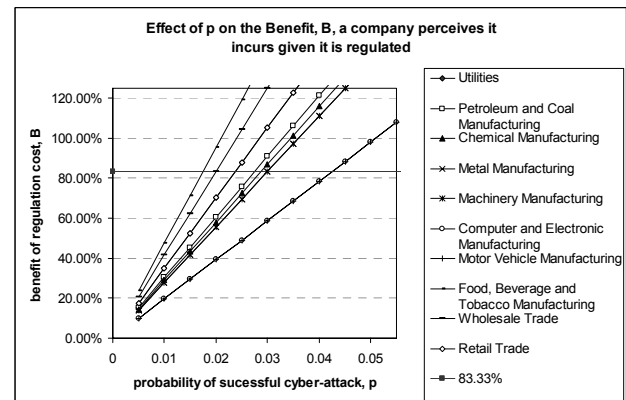


Fig. 3. This shows a positive relationship, in all industries, between p and B. Companies would voluntarily choose (without being regulated) to invest in cyber-security for B equal to 83.33%. For different industries, this occurs at widely different probabilities. Fig. 3 displays the value of incentives government would need to provide, in each industry, for firms to invest voluntarily in cyber-security, given a certain p.

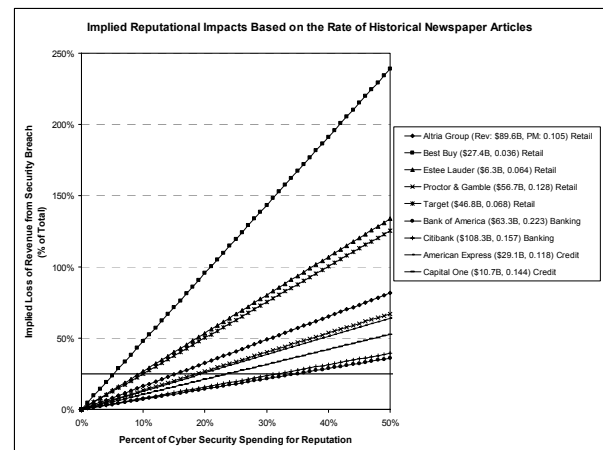


Fig. 4. Reputation Model Graph. This graph illustrates the percent of cyber security spending for reputation versus expected loss of revenue from a security breach for all nine companies observed.

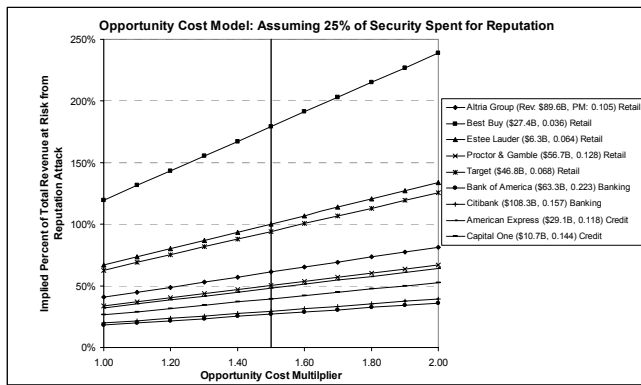


Fig. 5. Opportunity Cost Model Graph. This graph illustrates the implied percent of total revenue at risk from a reputation attack for all nine companies being examined. For this graph, the amount of cyber security spent for reputation is fixed at 25%. This is dependent on the opportunity cost multiplier.

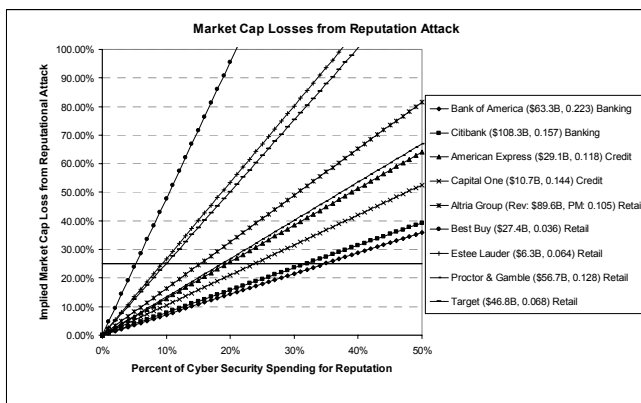


Fig. 6. Market Cap Loss Graph. This graph shows the implied market cap loss from a reputation attack based on the percent of market cap lost by security spent for reputation for the nine companies being studied.

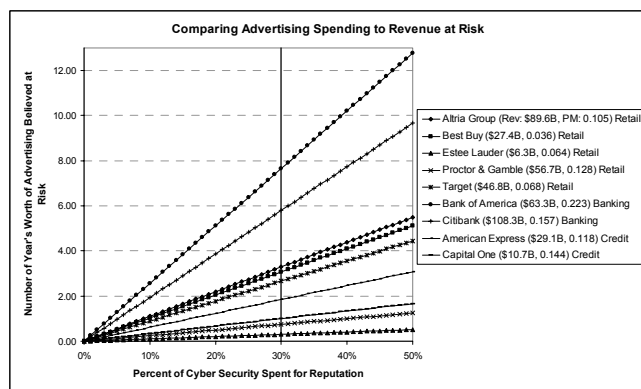


Fig. 7. Comparing Advertising Spending to Revenue at Risk Graph for Retail Sector. This graph illustrates the number of years' worth of advertising believed to be at risk from a security breach based on the percent of cyber security spent for reputation. This is shown for five retail companies.

REFERENCES

- [1] *The Economic Impact of the 182nd Airlift Wing Closure on Peoria, Woodford, and Tazewell Counties* (2005, Sept., 18). [Online]. Available: <http://www.peoriachamber.org/resource/166>.
- [2] Jackowitz. (2000). "CYBER-ATTACKS! Trends in US Corporations." *The Business Forum*. RAND Corporation. [Online]. <http://www.bizforum.org/whitepapers/rand001.htm>.
- [3] P. L. Kerstein. (2005, July, 19). "How Can We Stop Phishing and Pharming Scams?" *CSOnline.com*. [Online]. <http://www.csonline.com/talkback/071905.html>.
- [4] L. A. Gordon & M. P. Loeb. (2006). *Managing Cyber Security Resources*. New York: McGraw-Hill.
- [5] Cashell, W. D. Jackson, M. Jickling, B. Webel. (2004, April, 1). *The Economic Impact of Cyber-Attacks*. Congressional Research Service. The Library of Congress. [Online]. http://www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf.
- [6] *One Hundred Leading National Advertisers*. (2005). [Online]. Available: <http://www.adage.com/datacenter.cms>.
- [7] Yahoo Finance. (2005). [Online]. Available: <http://finance.yahoo.com/>
- [8] A. Bartels, (2003, Dec., 29). *US IT Spending Forecast for 2004 - Up 4 Percent, as Spending Outpaces IT Budgets*." Forrester Research, Inc. Forrester Research, Inc.
- [9] *A Chronology of Data Breaches Reported Since the ChoicePoint Incident*. (2006). Privacy Rights Clearinghouse. San Diego, California.
- [10] U.S. Census Bureau. (2003). [Online]. Available: <http://www.census.gov/>.
- [11] Computer Security Institute. (2005). *CSI/FBI Computer Crime and Security Survey*.
- [12] J. Rollins & C. Wilson. (2005, Oct., 20). *CRS Report for Congress, Terrorist Capabilities for Cyberattack: Overview and Policy Issues*.
- [13] Chairman and Ranking Member Subcommittee on Cybersecurity, Science, and Research & Development of the U. S. House of Representatives Select Committee on Homeland Security. (2004, Dec.). *Cyber Security for the Homeland*.
- [14] Cyber Security Industry Alliance. (2005, Dec., 13). *National Agenda for Information Security in 2006*.
- [15] D. Alderson, K. Soo Hoo. (2004, Nov.). Stanford University's Center for International Security and Cooperation. *The Role of Economic Incentives in Securing Cyberspace*.
- [16] CRS Report for Congress. (2004, April, 16). *Computer Security: A Summary of Selected Federal Laws, Executive Orders, and Presidential Directives*.
- [17] E. Löwinder. (2005, Sept., 14). ".se is The First TLD in The World with DNSSEC - A More Secure Technique for Name Resolving on the Internet." *Press Releases*. Network Information Centre Sweden AB. [Online]. <http://www.nic.se/english/nyheter/pr/>.
- [18] NIC-SE. (2005). DNSSEC – What is it and what does it do? [Online]. www.nic.se.
- [19] S. Schechter & A. Ozment. (2006). *Least Cost Paths to Deployment of Infrastructure Security Technologies*. Lincoln Laboratory. Massachusetts Institute of Technology.
- [20] J. Evers. (2006, March, 24). DNS servers do hackers' dirty work. *CNET News.com*. [Online]. <http://news.com.com/>.
- [21] R. Vaughn & G. Evron. (2006, March, 17). *DNS Amplification Attacks*, Baylor University. pp. 2-3.
- [22] Berlind. (2003, Aug. 7). DNS Inventor Says Cure To Net Identity Problems Is Right Under Our Nose. *CNET News.com*. [Online]. <http://techupdate.zdnet.com/>.
- [23] R. Lemos. (2005, April, 8). DNS Attacks Attempt To Mislead Consumers. *SecurityFocus*. [Online]. Available: <http://www.channelregister.co.uk/>.