CRS Report for Congress

Received through the CRS Web

The Economic Impact of Cyber-Attacks

April 1, 2004

Brian Cashell, William D. Jackson, Mark Jickling, and Baird Webel
Government and Finance Division

The Economic Impact of Cyber-Attacks

Summary

Information security – the safeguarding of computer systems and the integrity, confidentiality, and availability of the data they contain – has long been recognized as a critical national policy issue. Its importance is growing as the integration of computers into more and more aspects of modern life continues. In addition, cyber-attacks, or breaches of information security, appear to be increasing in frequency, and few are willing to ignore the possibility that the severity of future attacks could be much greater than what has been observed to date.

A central issue, in both public and private sectors, is whether we are devoting enough resources to information security. Part of the answer must come from economic analysis. What are the costs, both historical and potential, of security breaches? How frequently can attacks be expected? Can these factors be quantified precisely, so that organizations can determine the optimal amount to spend on information security and measure the effectiveness of that spending?

No one in the field is satisfied with our present ability to measure the costs and probabilities of cyber-attacks. There are no standard methodologies for cost measurement, and study of the frequency of attacks is hindered by the reluctance of organizations to make public their experiences with security breaches. This report summarizes the limited empirical data on attack costs, and surveys recent theoretical work that seeks to overcome the absence of reliable and comprehensive statistics.

Investigations into the stock price impact of cyber-attacks show that identified target firms suffer losses of 1%-5% in the days after an attack. For the average New York Stock Exchange corporation, price drops of these magnitudes translate into shareholder losses of between $50 million and $200 million.

Several computer security consulting firms produce estimates of total worldwide losses attributable to virus and worm attacks and to hostile digital acts in general. The 2003 loss estimates by these firms range from $13 billion (worms and viruses only) to $226 billion (for all forms of overt attacks). The reliability of these estimates is often challenged; the underlying methodology is basically anecdotal.

The insurance industry's response to rising perceptions of cyber-risk has been twofold. Initially, most companies excluded, and continue to exclude, cyber-attacks from standard business insurance coverage. After this initial exclusion, several insurers then began selling specialized cyber-risk policies. Growth of the market has been slow; lacking the empirical data to construct actuarial tables, insurers are unable to price risk with the degree of confidence they enjoy in traditional insurance lines.

Estimates of the macroeconomic costs of cyber-attacks are speculative. As long as any cyber-attack is limited in scope and short-lived it is likely that macroeconomic consequences will be small. But the ability to recover quickly is important, since the length of time computers are affected is an important determinant of the costs. It may be almost as important for firms to address their abilities to restore operations as to insulate themselves from potential attacks.

This report will not be updated.

Contents

List of Figures

List of Tables

The authors wish to express their appreciation to David Brumbaugh, Walter Eubanks, and Maxim Shvedov of the Government and Finance Division, who provided valuable advice on several key points, but are in no way responsible for any shortcomings that remain.

The Economic Impact of Cyber-Attacks

The importance of electronic information systems is obvious to all participants in the modern economy. When information fails to circulate, whole sectors of the economy are vulnerable. Finance, wholesale and retail trade, transportation, much of manufacturing, and many service industries would slow to a crawl without computers. Vital public services – utilities, national defense, and medicine – are equally dependent.

Information security – the safeguarding of computer systems and the integrity, confidentiality, and availability of the data they contain – has long been recognized as a critical national policy issue. Two current trends indicate that its importance is growing. First, the integration of computers into more and more aspects of modern life continues. Second, cyber-attacks, or breaches of information security, appear to be increasing in frequency, and few observers are willing to ignore the possibility that future attacks could have much more severe consequences than what has been observed to date.

The core issue, in both public and private sectors, is whether we are devoting enough resources to information security. Part of the answer must come from economic analysis. What are the costs, both historical and potential, of security breaches? How frequently can attacks be expected? Can these factors be quantified precisely, so that business firms and other organizations can determine the optimal amount to spend on information security and measure the effectiveness of that spending?

This report surveys the state of knowledge on the cost of cyber-attacks and the economics of information security. First, we summarize several studies that use stock market capitalization as a measure of the cost of cyber-attacks to victim firms. The studies find substantial short-term drops in the prices of shares of firms following the announcement of an information security breach: between 1% and 5% of market capitalization, with greater losses (up to 15%) recorded by some financial institutions where attackers had gained access to confidential customer records.

Second, we present summaries of the existing empirical data on costs attributable to cyber-crime and computer worms and viruses. What is available is a limited amount of survey data, which is frankly described by its compilers as anecdotal, but is nonetheless widely reported in the press.

Third, we analyze the reasons for the lack of statistical data: firms and organizations have strong incentives to conceal information about cyber-attacks, and there are significant uncertainties and measurement difficulties that limit our ability to specify the dollar amount at risk from information security breaches. Theoretical models that describe the returns to spending on information security shed some light on the size of potential losses, but – in the absence of better statistical data – assigning an overall figure to the cost of cyber-attacks remains highly speculative.

Fourth, we examine the efforts of the insurance industry to develop policies that cover cyber-risk. These initiatives are in their infancy; the chief obstacle has been a lack of data with which to construct actuarial tables on the costs and frequency of attacks.

Finally, we consider cyber-attacks as macroeconomic events.

Appendices to this report include a summary of information risk assessment practices in a Fortune 500 manufacturing company and an overview of efforts by financial institutions and regulators to manage cyber-risk in that industry.

Studies of the Effect of Cyber-Attacks on Stock Prices

Thus far, reported cyber-attacks have been relatively limited in scope, and have not yet been on a scale that would have significant macroeconomic consequences. Individual firms, however, may have suffered significant losses as a result of past attacks. An examination of the effects of those attacks might be illuminating. Most estimates of the cost to companies of cyber-attacks are based on surveys. Survey responses are often expressed in such a wide range as to indicate considerable subjectivity and thus they may be of limited use. There may, however, be a more objective measure of the effect of cyber-attacks on individual firms.

In theory, the price of a company's stock is primarily determined by the present discounted value of the cash flows expected to result from that firm's output. That cash flow is what contributes to the wealth of the stockholders, either in the form of dividends or in the expansion of the firm's stock of productive capital. Any event that changes investors' expectations about that future stream of income is likely to affect the price of the stock.

Four recent studies have examined a number of actual cyber-attacks in an effort to see if any of those attacks could be linked to a change in the stock prices of the affected companies. In some cases, the studies attempted to measure if any stock-price effect depended on the different characteristics of either the firm or the attacks.

It seems at least intuitively obvious that some firms are more exposed to cyber-attacks than are others. It is conceivable that firm size may affect vulnerability to attack, but more to the point some firms are more dependent on computer networks than others to conduct business.[1] Conventional firms, which have been referred to in this context as "brick and mortar" firms, might be expected to be the least vulnerable to cyber-attacks as they are the least dependent on the Internet to conduct business. Some firms, characterized as "click and mortar," conduct business both off-line and over the Internet. These firms face an increased vulnerability because of the risk that the business they conduct via the Internet might be interrupted.

---

[1] This discussion draws on: Huseyin Cavusoglu, Birendra Mishra, and Srinivasan Raghunathan, "The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers," *International Journal of E-Commerce*, forthcoming, p. 57.

Finally, there are firms whose business is conducted almost exclusively over the Internet. These firms would seem to be most at risk.

The extent to which a business is affected might reasonably be expected to depend on the type of attack. Most attacks have fallen into one of two categories. The first is a "denial-of-service" attack (DoS). A DoS attack renders a firm's Internet portal inaccessible and interferes with its ability to conduct on-line business. For the most part, this kind of attack causes no lasting harm. The more serious category of attacks are those that involve the theft or destruction of secure information. This kind of security breach is more likely to have lasting effects on the targeted firm.

Other things being equal, the more dependent a firm is on the Internet, and the more intrusive an attack is, the more likely it is that any attack will have significant consequences for the financial health of that firm. Table 1 summarizes these considerations.

Table 1. Potential Financial Consequences of a Cyber-Attack

Type of Firm	Type of Attack	
	DoS	Security Breach
Conventional Brick and Mortar (e.g., Coca-Cola)	Lowest	
Click and Mortar (e.g., Borders)		
Internet Firms (e.g. Amazon, E-bay)		Highest

It might be expected in a study of the effects of past attacks that a pure Internet company whose network security is breached would suffer more than would a conventional firm that is affected by a DoS attack. But, it might also be presumed that those firms are fully aware of their respective vulnerabilities and so they allocate resources to computer security to differing degrees.

In contrast, firms that provide computer security might be expected to benefit from cyber-attacks (unless their products were publicly blamed for an attack's success). An increase in the apparent vulnerability of computer networks could be expected to raise future earnings of those companies and thus boost their stock price.

Cavusoglu, et. al., examined five specified hypotheses regarding the consequences of cyber-attacks.[2] To do so, they identified 66 distinct security breaches that occurred between 1996 and 2001. Of those 66 events, 34 were availability (DoS) attacks. Of the 66 events, 31 affected firms whose business was conducted almost entirely over the Internet.

---

[2] Ibid.

First, the study found, using the entire set of observations, that firm value was negatively affected by Internet security breaches. Firms affected by the attack experienced a 2.1% decline in value, relative to unaffected firms.

Second, the authors also found that firms that rely on the Internet for conducting business were more affected than were more conventional firms. Internet firms affected by an attack experienced a 2.8% decline in value relative to the other firms that were studied.

Third, the study found that smaller firms tended to lose more than did larger firms as the result of an attack.

Fourth, the kind of attack seemed to make no significant difference. A DoS attack was not found to be any less costly than an attack where there was a more severe breach in security.

Finally, the authors found that following the announcement of an attack, computer security firms experienced a 1.4% increase in market value, relative to other firms.

Campbell, et. al., examined 43 attacks, affecting 38 firms, which occurred between 1995 and 2000.[3] Looking at stock prices over a three-day period centered on the attack, they found that there was a significant, if modest, decline in the market values of affected firms as a result of the attack. The authors separately examined those attacks that did not involve unauthorized access to confidential data and those that did. They found that there was a significantly larger response in the latter type of attack. Those instances accounted for the significance of the overall effects. The stock price reaction to attacks which did not involve unauthorized access to confidential information was insignificant. The study concluded that investors, apparently, do not consider DoS attacks to be important, with respect to the long-run profitability of firms.

Ettredge and Richardson examined the effects of DoS attacks against Internet firms that occurred in February 2002.[4] This study examined the behavior of the stock prices of over 100 Internet-only firms, during a three-day window centered on the day of the DoS attack. Specifically, the authors wanted to know if the costs of an attack were greater for those firms that had a greater dependence on the Internet. They found that, on average, as a result of the February 2002 attack Internet firms lost 5% more in market value than did non-Internet firms, immediately following the attack.

Ettredge and Richardson also looked to see if there were differences among Internet firms. Using sample data describing different firms' own assessment of the

---

[3] Katherine Campbell, Lawrence A. Gordon, Martin P. Loeb, and Lei Zhou, "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence From the Stock Market," *Journal of Computer Security*, vol. 11, issue 3, 2003, pp. 431-448.

[4] Michael Ettredge, and Vernon J. Richardson, "Assessing the Risk in E-Commerce," *Proceedings of the 35th Hawaii International Conference on System Sciences - 2002*, p. 11.

risks they face due to conducting "e-commerce," the authors examined if those assessments were correlated with the loss following the February 2002 attack. The authors found that variations in perceived exposure to risk were correlated with variations in the loss of market value. The authors suggest that is evidence investors are able to distinguish among Internet firms based on their vulnerability to a cyber-attack.

Garg, et. al., studied 22 events that occurred between 1996 and 2002.[5] The authors determined that as a result of those attacks, the affected firms experienced a 2.7% decline in their stock price relative to the overall market on the day following the attack. Three days after the attack the stock prices of the affected firms had dropped 4.5%, relative to the rest of the market.

The attacks were divided into four distinct types: simple web site defacing; DoS; theft of credit card information; and theft of other customer information. In the case of web site defacing, the average loss in stock value was 2% on the second day, which rebounded somewhat to a 1.1% loss on the third day. DoS attacks resulted in a 2.9% drop on the second day, and a 3.6% decline on the third day. For attacks that compromise non-financial information, there was an average drop in stock value of 0.5% on the day of the attack, and a total decline of 1.5% on the third day. Attacks which compromised financial information, chiefly credit card data, caused the largest declines. On the day of the attack, stock prices of affected firms fell a average of 9.3% and by the third day the decline reached 15%. The authors also found that there was a correlation between the number of credit cards that were compromised and the magnitude of the stock price hit.

All the studies found that there was a significant decline in stock prices of affected firms in the days immediately following a cyber-attack. The time frame is necessarily restricted in an effort to isolate the effects of the attack. To extend the time horizon would increase the likelihood that any variation in stock prices was due to other events. Therefore, the studies do not attempt to determine if there is any persistent change in stock prices, or if the drop in stock prices is temporary.[6]

Two of the studies determined that the drop in stock price was related to the type of attack, with DoS attacks generally having a smaller effect than attacks which compromised confidential information. One of the studies found that there was no significant correlation between the kind of attack and the magnitude of the effect on stock prices. The fourth study found that the magnitude of the drop in price of stock was correlated with managers' assessments of the firm's exposure to the risk of cyber-attacks. Table 2 summarizes the findings.

---

[5] Ashish Garg, Jeffrey Curtis, and Hilary Halper, "Quantifying the Financial Impact of IT Security Breaches," *Information Management & Computer Security*, vol. 11, no. 2., pp. 74-83.

[6] Neither do any of the studies address differences among firms in how much they spend on computer security.

Table 2. Summary Findings of Stock Market Studies

	Does attack cause drop in stock price?	Does type of attack matter?
Cavusoglu, et. al.	-2.1% overall	no
Campbell, et. al.	significant modest decline	yes
Ettredge & Richardson	-5% (DoS only)	N.A.
Garg, et. al.	web site defacing: -1.1% DoS: -3.6% non financial info: -1.5% financial info: -15%	yes

Source: Studies cited in text.

How significant are these percentage drops in dollar terms? At the end of 2003, the average market capitalization (stock price times number of shares outstanding) for a company listed on the New York Stock Exchange (NYSE) was about $4.4 billion; for a company traded on Nasdaq, it was $870 million. A 2% drop in market capitalization is equivalent to an average dollar loss of about $88 million for an NYSE firm and about $17 million for a Nasdaq company.[7]

Survey Data on Cyber-Attack Costs

CSI[8]/FBI Computer Crime and Security Survey

In 2003, the Computer Security Institute (CSI) and the Federal Bureau of Investigation (FBI) published their eighth annual survey on computer crime and security. Computer security practitioners in 530 U.S. corporations, financial institutions, government agencies (federal, state, and local), medical institutions, and universities provided information about their organizations' experience with computer crime over the previous year.[9]

In 2003, 56% of respondents reported some unauthorized use of computer systems within the last 12 months. No such unauthorized use was reported by 29%, and 15% did not know. Figure 1 below shows the 2003 data on the percentage of respondents reporting various types of misuse and attacks, and the expected dollar value of losses by type attack. (Not all respondents provided dollar figures, as is discussed below.)

---

[7] It must be remembered that these are not out-of-pocket losses to the target firms, but paper losses spread over thousands of investors. Market capitalization is simply the stock market's implicit estimate of a company's total value at any point in time.

[8] The Computer Security Institute (CSI) is a membership organization for computer security professionals. CSI's activities include educational and advocacy programs.

[9] The 2003 survey is available online at [http://www.gocsi.com].

Figure 1. Types of Attacks Reported, and the Dollar Value of Related Losses, in the 2003 CSI/FBI Survey

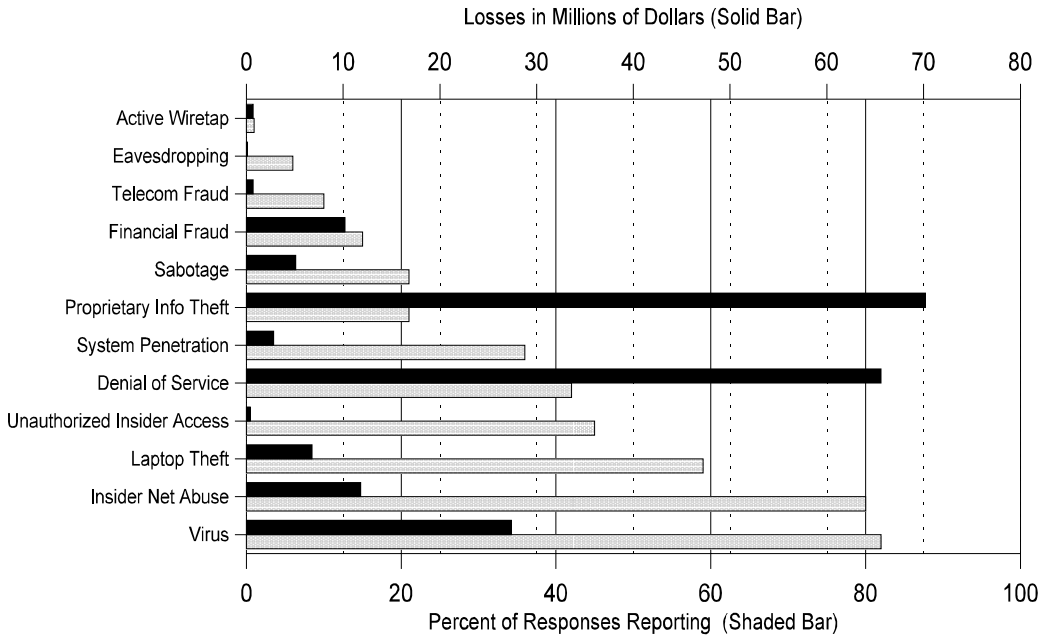


Figure 1 shows that the types of attacks most frequently reported are not the ones that cause the greatest losses. Theft of proprietary information (reported by 21% of respondents) and denial of service (reported by 42%) accounted for 67.3% of total reported money losses ($135.8 million out of $201.8 million).

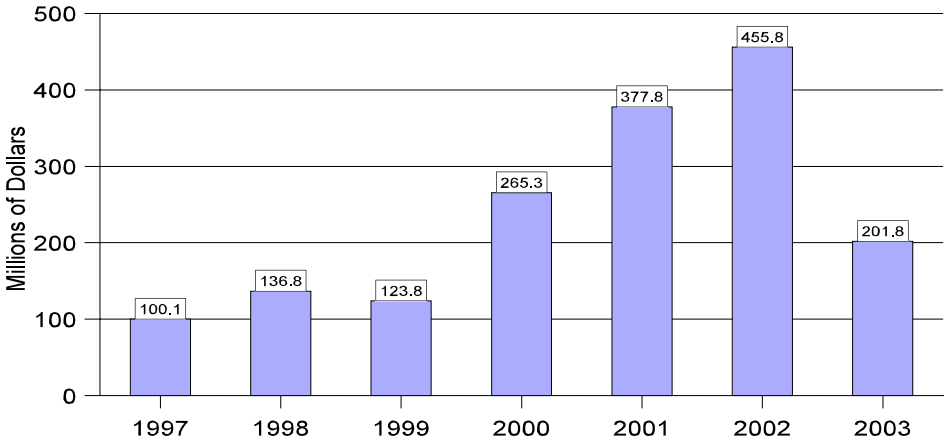
The distribution of losses by type of attack has not been consistent over the years that the survey has been conducted. In the 2000 survey, for example, theft of proprietary information was the most expensive type of attack, as it was in 2003. However, financial fraud accounted for 21.1% of all losses reported in 2000, as opposed to only 5.0% in 2003.[10]

There is no consistent trend in total reported financial losses to computer crime, as Figure 2 shows. It is likely that the results are skewed from year to year by a small number of relatively large loss reports. In addition, the number of respondents varies from year to year.

The survey also presents data on the reported costs of individual attacks, with highest, lowest, and average values, by type of incident. For 2003, the lowest cost reports drop into the hundreds of dollars; the highest values range up to $35 million (theft of proprietary information) and $60 million (denial of service).

[10] *2003 CSI/FBI Computer Crime and Security Survey*, p. 20.

Figure 2. Cost of Computer Crime As Reported in the CSI/FBI Surveys, 1997-2003



Besides the cost and frequency of attack data summarized here, the CSI/FBI surveys include information on incidents related to web sites, computer security practices, and the sources and methods of attacks.

What do the CSI/FBI survey results have to tell us about the overall costs of cyber-attacks in the United States? Unfortunately, not much. The survey's authors do not claim that their respondents are a representative sample of the businesses, organizations, and other entities that are exposed to cyber-risk.[11] Survey recipients are not randomly chosen, but are self-selected from among security professionals. As a result, there is no rigorous, statistically sound method for extrapolating the loss reports of the 530 respondents to the national level.

Secondly, the cost data reported are incomplete even for the sample. As noted above, 15% of respondents to the 2003 survey did not know whether there had been unauthorized use of their systems. More significantly, while 75% of respondents reported financial losses, only 47% could quantify the losses.[12] Thus, the figures in the charts above represent only measurable losses, and substantially understate total losses, though no one can specify the degree of understatement. Furthermore, if less than half of respondents reporting losses can put a dollar figure on those losses, the clear inference is that there is no standard technique for quantifying the amount of loss.

The survey does provide numerical support for a number of propositions that are generally accepted in the computer security literature: that insiders are the source of a substantial percentage of attacks;[13] that many attacks are unreported;[14] and that there is no simple, standardized method for quantifying the costs of cyber-attacks.

---

[11] Ibid., p. 18-19.

[12] Ibid., p. 20.

[13] Ibid., p. 7 and 9.

[14] Only 30% of organizations that experienced computer intrusions reported them to the police, and only 21% reported intrusions to legal counsel. Ibid., p. 18.

Although limited as a statistical tool, the surveys usefully provide, in the authors' own words, "a series of snapshots of how the people in the trenches viewed their situation at a given time."[15]

Figures on Worldwide Costs of Viruses, Worms, and Other Attacks

The cyber-attack cost figures most often reported in the media come from two computer security consulting firms, Computer Economics Inc. and Mi2g.[16] These firms are not primarily research organizations; their data are not published freely, but are available only to subscribers and clients. The figures presented below are derived from press accounts and from a limited amount of material made available to CRS on a courtesy basis.

Computer Economics Inc.

Computer Economics (CEI), based in Carlsbad, California, has for several years published estimates of the financial costs of malicious code attacks – viruses, worms, and the like. The table below presents CEI estimates for the worldwide costs of major virus attacks between 1995 and 2003.

Table 3. Annual Financial Impact of Major Virus Attacks, 1995-2003

Year	Cost ($ billions)	Year	Cost ($ billions)
1995	0.5	2000	17.1
1996	1.8	2001	13.2
1997	3.3	2002	11.1
1998	6.1	2003	12.5
1999	12.1		

Source: Computer Economics Inc. *Security Issues: Virus Costs Are Rising Again.* September 2003, p. 3. (Note: 2003 figure is an estimate based on January through August data.)

How does CEI calculate these figures? Its basic data sources, as described in a Cisco Systems study,[17] include the following: data collected from its own clients

---

[15] Ibid., p. 20.

[16] For overviews of these companies, see: [http://www.computereconomics.com] and [http://www.mi2g.co.uk], respectively.

[17] *Economic Impact of Network Security Threats,* Cisco Systems, Inc. White Paper, 2002, (continued...)

and other organizations around the world, review of statistical reports and studies, surveys of security practices and spending, and the activity reports of security companies. The firm has developed benchmarks to measure the costs of recovery and cleanup after attacks, lost productivity, and lost revenue from downtime. These benchmarks underpin a model that permits extrapolation from the data CEI collects to an estimate of the worldwide costs of malicious code attacks.

Mi2g.

Mi2g, a British firm, publishes estimates of the costs of worm, virus, and other malicious software (which it calls "malware") attacks. In addition, the firm publishes figures on the incidence and costs of a broader category of cyber-attack, which it calls "overt digital attacks."[18] The number of such attacks reported has gone from near zero in the mid-1990s (4 attacks reported in 1995) to about 200,000 in 2003.[19] Cost estimates for digital attacks, including hacking, malware, and spam, are shown in table 4 below. The estimated costs include business interruption, denial of service, data theft or deletion, loss of sensitive intelligence or intellectual property, loss of reputation, and share price declines.

Table 4: Worldwide Economic Damage Estimates for All Forms of Digital Attacks, 1996-2004

Year	Cost ($ billions)		Year	Cost ($ billions)	
	Lower	Upper		Lower	Upper
1996	0.8	1.0	2001	33	40
1997	1.7	2.9	2002	110	130
1998	3.8	4.7	2003	185	226
1999	19	23	2004	46	56
2000	25	30			

Source: Mi2g, *Frequently Asked Questions: SIPS and EVEDA, v1.00,* updated February 6, 2004. (2004 data are on a "so far" basis.)

---

[17] (...continued)
p. 16.

[18] Mi2g defines an overt digital attack as one in which a hacker group gains unauthorized access to a computer network and modifies any of its publicly visible components. Overt attacks may include either data attacks, where the confidentiality, authenticity, or integrity of data is violated, or control attacks, where network control or administrative systems are compromised. Overt attacks are those that become public knowledge, as opposed to covert attacks, which are known only to the attacker and the victim.

[19] Mi2g, *SIPS Report,* November 2003, p. 8.

For the full year 2004, Mi2g has projected that worldwide economic damage from digital attacks will exceed $250 billion.[20] This figure may be out of date: the firm has reported that February 2004 was the most costly month in history, with economic damage estimated at $83 billion.[21]

A document on the company's website[22] lists the following sources of data: personal relationships with banks, insurers, and reinsurers; monitoring hacker bulletin boards and hacker activity; and anonymous channels to "black hat" hacker groups. Economic information is collected from a variety of open sources and extrapolated to the global level using a proprietary set of algorithms. These algorithms, like CEI's benchmarks, are the key to the economic cost estimates. Since these models are proprietary, and based in large part on the consulting firms' contacts and experience in the IT security field, outside researchers cannot evaluate the models and their underlying assumptions.

These published figures are characterized as the firms' best estimates. Both firms are vendors of security services. The acceleration of costs since the mid-1990s, as reported by both CEI and Mi2g, is considerably more pronounced than the results of the CSI/FBI survey would suggest. Between 1997 and 2003, attack or crime costs either doubled (according to CSI/FBI data), quadrupled (according to CEI), or went up a hundredfold (Mi2g). Of course, the surveys are not measuring identical sets of phenomena, but the variation suggests how far we are from a standard method of quantification of these costs.

Table 5 below presents cost data for specific worm and virus attacks from both CEI and Mi2g. For some attacks, the estimates are very close; for others, they diverge sharply. The differences may reflect either differences in cost estimation models, or the two firms may define the episodes differently. (For example, one may break out cost figures for a number of separate attacks which the other regards as a single episode and produces a larger, consolidated cost estimate.)

---

[20] Bien Perez, "Defence Key as Digital Hazards Accelerate," *South China Morning Post,* Jan. 6, 2004, p. 3.

[21] Tim Lemke, "Computer Viruses, Worms Set Costly Internet Record," *Washington Times*, March 1, 2004.

[22] Mi2g, *Frequently Asked Questions: SIPS and EVEDA, v1.00,* updated Mar. 17 2004, see [http://www.mi2g.com/cgi/mi2g/press/faq.pdf] visited Mar. 31, 2004.

Table 5. Estimated Costs of Selected Virus and Worm Attacks, 1999-2003

(in billions of dollars)

Attack	Year	Mi2g	CEI
SoBig	2003	30.91	1.10
Slammer	2003	1.05	1.25
Klez	2002	14.89	0.75
BadTrans	2002	0.68	0.40
Bugbear	2002	2.70	0.50
Nimda	2001	0.68	1.50
Code Red	2001	2.62	2.75
Sir Cam	2001	2.27	1.25
Love Bug	2000	8.75	8.75
Melissa	1999	1.11	1.10

Sources: Mi2g figures: Richard Waters, "When Will They Ever Stop Bugging Us?" *Financial Times*, September 17, 2003, special report, p. 2 (The figures in this table average Mi2g's upper and lower estimates.); CEI figures: Computer Economics Inc. *Security Issues: Virus Costs Are Rising Again.* September 2003, p. 2.

Other IT firms and organizations, including TrendMicro, Jupiter Media Matrix, and Britain's IT Corporate Forum, produce estimates of the cost of virus and other attacks. While they do not publish time series or descriptions of their methodologies, their estimates are likely similarly derived – by extrapolation from a relatively small sample of cases based on their best judgement of how computer users worldwide are affected. Essentially, these estimates constitute anecdotal rather than statistical evidence.

Why Empirical Data Are Scarce

Accurate and statistically comprehensive data on the incidence and costs of cyber-attacks are critical to the analysis of information security. Nevertheless, as a 2002 World Bank study found, "the existing base of information that supports projections about the extent of the electronic security problem is substantially flawed."[23] If information gathering has the potential to reduce costs and risks, why does the data shortfall persist?

---

[23] Thomas Glaessner, Tom Kellerman, and Valerie McNevin, *Electronic Security: Risk Mitigation in Financial Transactions*, World Bank, June 2002, p. 16.

There are two chief obstacles. First, there are strong incentives that discourage the reporting of breaches of information security. Second, organizations are often unable to quantify the risks of cyber-attacks they face, or even to set a dollar value on the cost of attacks that have already taken place. Thus, even if all the confidential and proprietary information that victims have about cyber-attacks were disclosed and collected in a central database, measurement of the economic impact would still be problematical.

Incentives to Not Reveal Information

Comprehensive data on information security breaches are lacking not because the value of such data is not generally recognized. The problem is that organizations have real economic incentives not to reveal such information. The costs of public disclosure may take several forms:

- *Financial market impacts*. The stock and credit markets and bond rating firms may react to security breach announcements. Negative reactions raise the cost of capital to reporting firms. Even firms that are privately held, and not active in public securities markets, may be adversely affected if banks and other lenders judge them to be more risky than previously thought.

- *Reputation or confidence effects.* Negative publicity may damage a reporting firm's reputation or brand, or cause customers to lose confidence. These effects may give commercial rivals a competitive advantage.

- *Litigation concerns.* If an organization reports a security breach, investors, customers, or other stakeholders may use the courts to seek recovery of damages. If the organization has been open in the past about previous incidents, plaintiffs may allege a pattern of negligence.

- *Liability concerns.* Officials of a firm or organization may face sanctions under federal laws such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Gramm-Leach-Bliley Act of 1999 (GLBA), or the Sarbanes-Oxley Act of 2003, which require institutions to meet various standards for safeguarding customer and patient records.

- *Signal to attackers.* A public announcement may alert hackers that an organization's cyber-defenses are weak, and inspire further attacks.

- *Job security.* IT personnel may fear for their jobs after an incident and seek to conceal the breach from senior management.

Any of these disclosure costs can be significant. They may swiftly follow a public announcement and are borne by single firms or individuals within those firms. On the other hand, the presumed benefits of improved disclosure – improved efficacy and cost savings in data security – are likely to be slow to arrive and to be

diffused among many firms (including competitors). The imbalance between costs and benefits results in a market failure: individuals and organizations acting rationally in their own self-interest are unwilling to support an activity that would be beneficial to all if undertaken collectively. Gal-Or and Ghose construct a game theory model to show that information sharing would yield direct and indirect benefits to firms and industries and increase social welfare.[24]

In standard economic theory, a market failure represents an equilibrium state. Market participants following their individual interests will not change behavior that yields suboptimal outcomes unless some outside stimulus is applied. The government has for several years tried to encourage information sharing. In 1998, Information Sharing and Analysis Centers (ISACs) were established in several critical infrastructure industries by executive order.[25] The CSI/FBI surveys represent another public/private initiative. In 2004, the Bureau of Justice Statistics and the Department of Homeland Security are planning a full-scale survey of 36,000 businesses nationwide to map computer attacks, with critical infrastructure as a focus. To date, such programs have had limited success in overcoming what has been called "the tremendous power of suppressive forces [that] prevent information sharing."[26]

The Census Bureau recently completed a pilot test of a computer security survey, and reports that fewer than half of the surveyed companies responded, despite the bureau's strong track record in protecting confidential information. More than three fourths of the companies willing to provide reasons for non-response listed the voluntary nature of the survey as the reason for not filing. Census draws the following conclusion:

> The Bureau of Justice Statistics and the Bureau of the Census are now re-thinking their options. It may be possible to redesign the collection instrument in ways that improve response. But, there are serious doubts about the potential success of such efforts without mandatory collection authority. The future of this collection effort is unknown.[27]

Measuring Costs

While organizations may have good reasons not to make public disclosures regarding security breaches, one would expect their incentives to measure the costs of such incidents internally to be strong. Without accurate cost data, how would organizations assess the cyber-risks they face, make rational decisions about how much to spend on information security, or evaluate the effectiveness of security efforts? In fact, there are no standard methods for measuring the costs of cyber-

---

[24] Esther Gal-Or and Anindya Ghose, *The Economic Incentives for Sharing Security Information*, Paper presented to the 2nd Annual Workshop on Economics and Information Security, University of Maryland, May 29-30, 2003.

[25] Presidential Decision Directive 63.

[26] Kevin Soo Hoo, *How Much Is Enough*? *A Risk-Management Approach to Computer Security*, Stanford University Consortium for Research on Information Security and Policy (CRISP) Working Paper, June 2000, p. 30.

[27] See:[http://www.census.gov/eos/www/css/css.html], visited Mar. 31, 2004.

attacks. Attacks produce many kinds of costs, some of which cannot be quantified easily, if at all. As a result, there is a presumed gap in private, internal data that mirrors the absence of public data on cyber-attack costs.

The costs associated with cyber-attacks can be divided into direct and indirect costs. Direct costs include the expenses incurred in restoring a computer system to its original, pre-attack state. Recovery from an attack will typically require extra spending on labor and materials; these are the easiest costs to measure. But even at this basic level of cost accounting, complexities may arise. If an attack leads to increased spending on IT security, to what extent are those costs attributable to the attack? If a planned upgrade in hardware or software is accelerated after an attack, should the upgrade be classified as a security cost?

Another set of direct costs arises from business interruption. These costs may include lost revenue and loss of worker productivity during the disruption. Lost revenues may be easily measured by reference to a pre-attack period, but this may not tell the whole story. Lost sales may be a transitory phenomenon, limited to the attack period (and possibly made up afterwards), or they may be long-term, if, for example, some customers switch permanently to competing firms.

Measurement of productivity loss is not always straightforward or uniform. Generally, this is not an added dollar cost: the workers are paid what they would have been paid anyway. Assigning a value to lost time depends on each individual organization's estimates of its own costs related to business opportunities forgone (during the disruption) or diversion of resources (during the recovery effort).

Another direct cost may involve the loss of value in information assets that are stolen, compromised, or otherwise degraded during an attack. Soo Hoo summarizes the difficulties in measurement that may arise here:

> [T]he value of an information asset is highly dependent upon who possesses the information. Sensitive commercial R&D information in the hands of a competitor is significantly more problematic than if it were in the hands of a Netherlands teenager. Time sensitivity can also complicate the valuation problem. For example, a password that expires in ten seconds is worthless after it has expired, but it is quite valuable during the ten seconds that it could be used to gain system access. Add to these difficulties the quantification challenges posed by intangible values, such as reputation, trust, embarrassment, etc., and the task of valuation quickly becomes a highly uncertain and potentially contentious enterprise.[28]

Attacks also have indirect costs, which may continue to accrue after the immediate damage has been repaired. Many indirect costs flow from loss of reputation, or damage to a firm's brand. Customers may defect to competitors, financial markets may raise the firm's cost of capital, insurance costs may rise, and lawsuits may be filed. Some of these cost factors are readily quantifiable, but other aspects of loss of trust or confidence are intangible and difficult to measure.

---

[28] Ibid., p. 40.

Some analysts regard these indirect, intangible costs as more significant than direct costs. Cavusoglu, Cavusoglu, and Raghunathan conclude that the inability to measure intangible costs leads many firms to grossly underestimate the costs of security breaches, and that this explains why estimates of incident costs reported in the CSI/FBI survey are much lower than the price of an attack on a major company would be in terms of stock market capitalization.[29]

Indirect costs of cyber-attacks may also include economic harm to individuals and institutions other than the immediate target of an attack. An attack on one firm's computer networks may affect other firms up and down the supply chain. When credit card data is hacked, or an internet service provider goes down, consumers suffer costs. From an accounting perspective, these do not count as costs to the target firm, but from a policy perspective they can be significant. The possibility of cascade effects – disruption spreading from computer to interlinked computer – is well-known, but we are far from being able to quantify the economic impact of an event of this type.

To a profit-seeking business, measurement of costs already incurred is useful primarily to the extent that it facilitates prevention or mitigation of future losses. In the cyber-security field, as elsewhere, risk assessment is primarily a forward-looking activity. It is no less important or necessary because certain costs cannot be quantified. The next section of this report discusses the cost models that firms and organizations use for cyber-risk.

Cyber-Risk Cost Models

It is normal for businesses to make decisions on the basis of incomplete information. In cyber-risk management, these decisions involve the amount to spend on information security and how to allocate that budget. Despite the gaps in data and measurement capabilities, businesses, government, and other organizations have strong incentives – both economic and legal – to develop risk management programs that are as robust as possible.

Early attempts to measure cyber-risk led to the annual loss expectancy (ALE) model, developed in the late-1970s at the National Institute for Standards and Technology (NIST).[30] ALE is a dollar figure, produced by multiplying the cost, or impact, of an incident (in dollars) by the frequency (or probability) of that incident. In other words, ALE considers security breaches from two perspectives: how much would such a breach cost, and how likely is it to occur? ALE combines probability and severity of attacks into a single number, which represents the amount a firm actually expects to lose in a given year.

---

[29] Hasan Cavusoglu, Huseyin Cavusoglu, and Srinivasan Raghunathan, "Economics of IT Security Management: Four Improvements to Current Security Practices," unpublished paper, p. 5.

[30] For historical accounts of how the ALE and subsequent models evolved, see: Howard E. Glavin, "A Risk Modeling Methodology," *Computer Security Journal*, v. 19, no. 3 (Summer 2003), pp. 1-2; and Soo Hoo, *How Much Is Enough?* pp. 4-12.

ALE has become a standard unit of measure for talking about the cost of cyber-attacks, but the model is not universally used to assess cyber-risk. The reasons why not are apparent: the ALE model assumes that cost impact and frequency of attack are known variables, when in fact they both resist quantification. The difficulties in cost measurement have been set out above, and similar uncertainties apply to efforts to specify the likelihood of an attack.[31] Attempts to calculate a value for ALE run afoul of "the unrealistic and time-wasting assumption of numerically precise information."[32]

If a precise calculation of amounts at risk is not feasible, what are the alternatives? Numerous methodologies that measure risk qualitatively, rather than quantitatively, are in use. A common practice is to rank information assets according to (a) how valuable they are and (b) how vulnerable they are to attack. The results, which can be displayed in a matrix with high-risk, high-value assets in one corner and low-risk, low-value assets in the opposite corner, may guide a firm's allocation of its IT security spending. Appendix A to this report, an overview of the risk assessment policies of a Fortune 500 manufacturing company, provides an illustration of such a qualitative ranking system.

A comprehensive survey of risk assessment methods is beyond the scope of this report. Worth noting, however, is one theme that emerges from a review of the information security literature: a drive to develop new methodologies that allow for the quantification of risk. Although the data needed to perform traditional business calculations, such as return on investment or cost/benefit analyses of security spending may be unavailable, "the urge to measure is everywhere."[33] The only alternative to developing new and better quantitative methods – expressed in a mordant acronym that occurs again and again – is said to be FUD, or "fear, uncertainty, and doubt." It has been proposed that IT security can borrow from models in use in other fields, such as industrial quality control, public health reporting, financial market portfolio management, accelerated failure testing in manufacturing, and insurance.[34] It remains to be seen whether avenues like these will lead to better measurement of cyber-risk.

IT Security Spending

For businesses facing cyber-risk, the "bottom line" question is how much to spend on information security. The difficulties in measuring risk set forth above

---

[31] The CERT Coordination Center and others publish raw data on the number of attacks, but these figures (which have been growing rapidly in recent years) do not distinguish between major and minor incidents. The data sharing problem discussed above hampers efforts to collect reliable figures on the frequency of attacks in the past, but such figures, even if available, might be of limited use if cyber-attacks are becoming more common, as the CERT data suggest.

[32] Love Ekenberg, Subhash Oberoi, and Istvan Orci, "A Cost Model for Managing Information Security Hazards," *Computers and Security*, v. 14, no. 8 (1995), p. 715.

[33] Dan Geer, "Risk Management Is Still Where the Money Is," *Computer Security*, Dec. 2003, p. 131.

[34] Daniel Geer, Jr., Kevin Soo Hoo, and Andrew Jaquith, "Information Security: Why the Future Belongs to the Quants," *IEEE Security and Privacy*, v.1, July/Aug. 2003, pp. 26-28.

translate into similar uncertainties regarding security spending. Security budgets cannot be justified through the basic financial tests – return on investment (ROI) and cost/benefit analysis – that are applied to most other corporate investments. It is hard to overstate the starkness with which this inability to quantify appears in the information security literature. As one observer stated:

> It's fairly easy to find out how many people die from smoking cigarettes in the United States each year. It's impossible to find out how many hours of computer downtime result from computer virus outbreaks in a year.
>
> It's fairly easy to find out how much physical money is stolen from banks in the United States each year. It's impossible to find out how much money is stolen from banks through electronic attacks.
>
> It's easy to find out how likely you are to be injured in a head-on accident in a particular kind of vehicle in the United States. It's impossible to find out how likely your server is to be taken offline by a virus attack.
>
> It's easy to find out how long a gun safe will resist the attentions of a thief armed with an acetylene torch. It's impossible to find out how long your server will resist the attentions of a thief armed with hacking tools publicly available on the Internet.
>
> A core problem of the information security industry is that, as an industry, we do not have a unit which measures product effectiveness. We are selling something which is intangible and unquantifiable; we are basically selling fashion rather than function.[35]

Of 1,400 organizations surveyed by Ernst & Young in 2003, 59% reported that they rarely or never made an ROI calculation for information security spending.[36] Nevertheless, all organizations must decide how much to spend.

Survey evidence shows that many organizations are spending increasing amounts on IT security. International Data Corp. (IDC) found that nearly 40% of organizations polled in 2003 reported that security spending was growing faster than general IT spending. For very large organizations, the proportion was 51%. Only about 10% reported that IT security spending was growing at a slower rate than IT spending.[37]

Rising security spending suggests that organizations perceive either an increase in risk or that past expenditures were inadequate to manage current risk. Does the level of IT security spending provide clues to the dollar amounts at risk from cyber-attacks?

---

[35] Bob Blakely, "The Measure of Internet Security Is Dollars", Paper presented at the Workshop on Economics and Computer Security, University of California, Berkeley, May 16-17, 2002.

[36] Ernst & Young LLP, *Global Information Security Survey 2003*, p. 8. (The survey is available online at: </www.ey.com/global/Content.nsf/International/Press_Release_-_2003_Global_Information_Security_Survey>.

[37] Brian E. Burke, et al., *IDC's Enterprise Security Survey, 2003*, Nov. 2003, p. 14.

Given the uncertainties in measuring costs, risks, and the effectiveness of security efforts, we cannot make simple statements like the following: a company that expects to lose *x* dollars per year to cyber-attacks will generally spend *y* dollars to mitigate those losses. Until better empirical cost data become available, such calculations will remain speculative.

However, theoretical models have been developed that attempt to shed some light on the returns to security spending. These models are fairly rudimentary, but as they are refined, or even in their present state, they may help put security spending decisions on a more rational and rigorous basis.[38]

The Smokestack Curve

The first observation from these theoretical models is that there are diminishing returns to security spending. A little spending can bring a substantial reduction in expected losses (ALE). At higher levels of spending, the reduction per dollar spent will be less. At very high levels, the extra amount of loss reduction purchased may be very low, or even approach zero. In graphic terms, this pattern is called a smokestack curve, resembling a plume of smoke rising vertically at first, then flattening out as it cools and drifts away on the wind.

Diminishing returns are observed in many business situations; Moitra and Konda provide evidence for them in security spending. They conduct a simulation of malicious attacks against network systems, and measure survivability – the degree to which a system is able to withstand attack and still function at a certain level – when different levels of defense mechanisms are deployed. Their results show survivability at various levels of security expenditure. They summarize their findings as follows:

> As cost increases, survivability increases rapidly at first, and then more slowly. Such a plot can provide a systems manager with the ability to make an informed decision about the level of defense that is most appropriate for his or her organization since it shows the tradeoff involved between cost and expected survivability.[39]

In Moitra and Konda's analysis, firms' security spending decisions will depend upon how risk averse they are. If a particular security breach will cause intolerable losses, firms may continue to spend on security even when the marginal return is low. Gordon and Loeb[40] introduce the assumption of risk neutrality, which means that the firm is indifferent to investments that have the same expected return, even

---

[38] Scott Berinato, "Finally, a Real Return on Security Spending," *CIO*, v. 15, Feb. 15, 2002, p. 43.

[39] Soumyo D. Moitra and Suresh L. Konda, *The Survivability of Network Systems: An Empirical Analysis*, Carnegie Mellon Software Engineering Institute (CMU/SEI-2000-TR-021), Dec. 2000, p. 27.

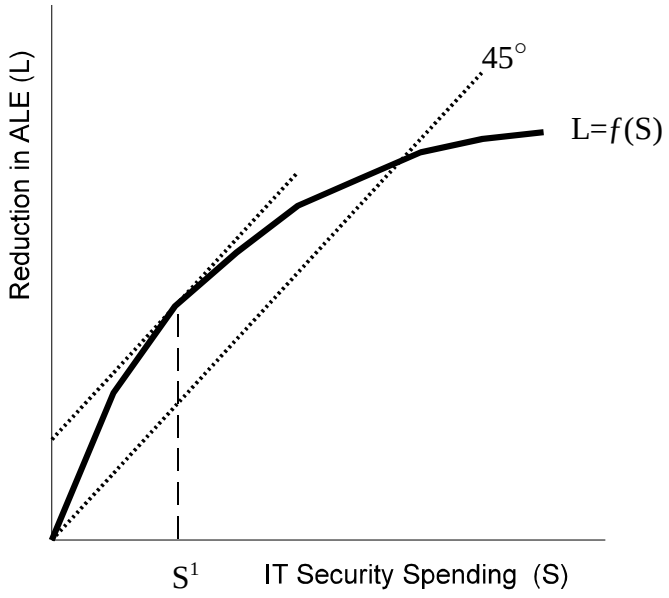
[40] Lawrence A. Gordon and Martin P. Loeb, *ACM Transactions on Information and System Security*, Nov. 2002, p. 438.

though the investments may have varying amounts of risk.[41] Under risk neutrality, a profit-maximizing firm would increase spending on IT security as long as the return (in terms of reduction in ALE, or expected loss) exceeded the marginal expenditure. The firm would stop spending when one additional dollar spent on security reduced ALE by less than a dollar.

By assuming risk neutrality, Gordon and Loeb identify an optimum level of security spending, found at the point on the smokestack curve where marginal security spending equals marginal loss reduction. This is shown in figure 3 below. The horizontal axis represents IT security spending (S); the vertical axis shows the amount by which ALE is reduced (L). The dotted line from the origin is a 45 degree line, along which an increase in S produces an equal increase in L. Optimal security spending (S^1) is determined by the point at which the slope of the flattening curve is 1 (where the change in L divided by the change in S equals one), or where the tangent of the curve is parallel to the 45-degree line. This point on the curve is also where the difference between benefits and costs is maximized.

Loeb and Gordon push this analysis further. By making several assumptions about the shape of the cost/loss reduction curve, they reach some numerical conclusions about the optimal level of security spending as a percentage of ALE:

Figure 3. Returns to IT Security Spending



Source: Chart by CRS, based on Gordon and Loeb, "The Economics of Information Security Investment."

[41] In IT security terms, risk neutrality would mean that the firm did not differentiate between a high-cost, low-probability event and a low-cost, high-risk attack. Clearly, this is a simplifying assumption that will not always hold true in the real world.

> Our analysis shows that for two broad classes of security breach probability functions, the optimal amount to spend on information security never exceeds 37% of the expected loss resulting from a security breach (and is typically much less than that 37%). Hence, the optimal amount to spend on information security would typically be far less than the expected loss from a security breach.[42]

Since Loeb and Gordon's model is theoretical and not based on empirical data, the nature of their assumptions determines their results. Without evaluating the robustness of their assumptions (or the completeness of the mathematical proofs of the propositions that flow from the assumptions), it may be interesting to see what their estimate of optimal IT security spending suggests for the value of ALE.

We can roughly estimate the amount spent on IT security, even though there is no standard definition of what constitutes security spending (as opposed to, for example, normal upgrades of hardware and software), and even though statistics based on direct measurement or reporting are not available. A common rule of thumb is that organizations devote roughly 5% of their total IT spending to IT security.[43] Forrester Research, Inc. projects that total IT spending by business and governments in the United States in 2004 will be $743 billion.[44] With these two assumptions, we can estimate that IT security spending by U.S. businesses and governments in 2004 will be about $37 billion.

Gordon and Loeb's model suggests that this figure does not exceed (and is probably considerably less than) 37% of ALE, or the amount organizations expect to lose as a result of cyber-attacks. Thus, a figure of $100 billion represents a lower bound estimate for the annual expected loss in the United States. To the extent that firms spend less than 37% of their expected loss on security, the estimated figure for ALE rises.

Is IT Security Spending Too High or Too Low?

Gordon and Loeb's model estimates an optimal level of security spending. There are arguments, however, that organizations do not now spend an optimal amount on security – that current spending is either too high or too low.

---

[42] Ibid., p. 453.

[43] Evidence for this comes mainly from surveys. See, e.g., George V. Hulme, "Companies Not Spending More on Security, Even With Increased Threats," *CMP TechWeb*, July 28, 2003 (companies spent 5.4% of their IT budget on security in 2003, according to Gartner Associates); Bob Violino, "Survey Report– The Security Team – IT Organizations Are Making Security a Primary Job Function," *Network Computing*, Sept. 25, 2003 (Secure Enterprise survey finds that 5% is the median security expenditure); Robert D. Austin and Christopher A.R. Darby, "The Myth of Secure Computing," *Harvard Business Review*, June 2003, p. 121 (the average company spends 5% to 10% of its IT budget on security); and Computer Economics Inc., *2003 Information Systems Spending*, p. 11-1 (security software and hardware alone account for 2.8% of total IT budgets).

[44] This figure includes hardware, software, consulting and services, outsourcing, and IT salary and benefits. Tom Pohlmann, et al., "CIOs Still Have Cautious Outlook for 2004 IT Budgets," *Business Technographics Brief Series*, Nov. 7, 2003, Figure 4.

Why would firms spend too much on security? One reason that is cited repeatedly is that some security spending is driven by legal and regulatory, rather than economic, considerations. Over 40% of respondents to IDC's 2003 security survey reported that "compliance with industry regulations" was the most important factor contributing to growth in IT security spending. Only about 25% cited "risk-level concern at executive level" as the most important factor.[45]

Another argument is that since many firms cannot perform a satisfactory return-on-investment calculation for security spending, they adopt a "best practices" approach and simply make the same kind of investments they see other firms making. Critics of this approach claim that the result is a herd mentality, leading to expenditure on security features that may be of little value to the buyer's specific needs. For example:

> Think about why firewalls succeeded in the marketplace. It's not because they're effective; most firewalls are installed so poorly as not to be effective, and there are many more effective security products that have never seen widespread deployment. Firewalls are ubiquitous because auditors started demanding firewalls.[46]

On the other hand, some companies regard existing security products and services as useful and desirable but not affordable. Many executives view security as an underfunded area. "Insufficient budget" was cited as the primary obstacle to effective information security by 56% of respondents to the Ernst & Young survey.[47] Similarly, "lack of resources" was most often named as the biggest challenge to security infrastructure management in the IDC security survey.[48]

Some analysts tend to discount these views: "Individuals who self-select into security professions may be those biased toward greater risk avoidance than are members of the general population, and thus might be prone to overestimate potential losses or willing to authorize greater prevention expenses than actually necessary."[49]

Given the lack of empirical data about cyber-attack costs and the measurement difficulties that have been discussed in this report, it is not surprising that there are different views on the appropriate level of security spending. A single dramatic security breach could produce a significant shift in risk perceptions. Nevertheless, there is no strong reason to think that firms consistently spend too much or not enough: over time, a competitive market ought to punish both those that overspend (and divert resources from more productive uses) and those that spend too little and suffer larger losses as a result. The amount of scarce resources actually allocated to

---

[45] *IDC's Enterprise Security Survey, 2003*, p. 15.

[46] Bruce Schneier, "Computer Security: It's the Economics, Stupid," Paper presented at the Workshop on Economics and Computer Security, University of California, Berkeley, May 16-17, 2002.

[47] *Global Information Security Survey 2003*, p. 9.

[48] *IDC's Enterprise Security Survey, 2003*, p. 16.

[49] Rebecca T. Mercuri, "Analyzing Security Costs," *Communications of the ACM*, v. 46, June 2003, p. 18.

security is a market judgement on the severity of cyber-risk, and it is hard to assume that arguments from theory or abstract principles can improve on that judgement.

Cyber-Attacks and the Insurance Industry

As an industry dedicated to accepting risks that people and businesses want or need to shed, the insurance industry is unsurprisingly interested in the increasing risk of cyber-attack. As these risks became larger and more evident with the growth of the Internet, the insurance industry's reaction was essentially two-fold. The initial reaction was largely to make it clear that existing business insurance did not include coverage of cyber-risks. The premiums charged for existing types of business insurance essentially did not account for the risk from some form of cyber-attack and thus to cover these risks at the existing lower premium rate would have been economically damaging to the insurance company. In general, the reaction of excluding a new risk once it becomes known is quite common in the insurance industry. One can see it, for example, in the reaction to the 9/11 attacks and in the industry's reaction to the increase of homeowners' claims for mold damage, particularly in Texas. In both cases, these risks were presumed to be included in policies when they were low frequency and low cost risks. Once it became clear that they were not such low frequency and low cost risks, insurance contracts began to specifically exclude them.

The second reaction to this new cyber-risk was to introduce specific policies to cover those risks that had been excluded from traditional business insurance coverage. This largely began occurring in 1999 although some coverage was offered as far back as 1997. The market leader in cyber- risk policies, AIG, is estimated to have approximately 70% of the market for cyber-risk insurance with approximately 2,500 policies issued.[50] Other companies writing policies include Chubb, St. Paul, Zurich American, Hartford, and Ace Ltd. The total premium for such policies has been estimated to be between $60 million and $120 million in 2002.[51] These numbers are, however, quite different compared to those found in other types of commercial insurance. For example, general business liability insurance premiums totaled more than $30 billion in 2002,[52] and AIG is able to lead the market for commercial lines with only 9% of the total commercial market in 2002.[53] Estimates for growth in cyber-insurance coverage are substantial, with the Insurance Information Institute seeing $2 billion in premiums by 2007 or 2008,[54] while Conning and Co. projects a 100% annual growth rate and a total premium volume as high as $6 billion by 2006.[55]

---

[50] Ron Panko, "Under Separate Cover," *Best's Review*, July 1, 2003, pg. 96-8.

[51] Ibid, p. 95.

[52] Insurance Information Institute, "Fact Book 2004," pp. 73-74

[53] Ibid, p. 71.

[54] See [http://www.iii.org/media/hottopics/insurance/computer], visited Mar. 11, 2004.

[55] See [http://www.conning.com/irpstore/PressReleases/020318.asp], visited Mar. 11, 2004.

The policies offered by the companies in this area vary greatly as to the terms and coverages. There is no standard cyber-insurance policy. Policies can include both first party and third party risks with most companies apparently showing a preference for covering third party risks before covering first party risks. This seems to be due to a faith that the computer systems under a company's direct control are sufficiently secured to prevent direct loss of company data or the like. Risks that can be covered include: network security (damage due to direct attack on a network/transmission of a virus/unauthorized access), web content (copyright infringement/libel or slander claims from material posted on a website), business interruption (lost income due to loss of computer function after an attack), cyber-extortion (settlement of an extortion attempt against a network), and public relations (cost of repairing a company's image after a cyber-attack).

The principal challenge facing the insurance industry in this realm is a lack of data. Insurance pricing rests critically on an understanding of the risks that are being transferred, particularly the frequency of the risk and the possible damages that could result. With enough experience and data, the insurance industry can be extremely accurate in its predictions and very efficient at dealing with risk, even with risks that might be very rare or very damaging. The risks to be covered by cyber-insurance, however, were not only unexpected, but also are to a large degree qualitatively different from what has been seen in the past. This leads to a situation where insurers are writing policies without the type of information that they prefer, particularly when compared to lines like fire or auto where insurers have long historical experience. AIG might estimate, as it has, that computer viruses caused $13 billion in damage in 2001. However, this would only be the beginning of the questions that might need to be answered. What is the likely frequency of such attacks? Is this number a high number or low number compared to what the costs might be in the future? What steps has a particular company taken to mitigate the damage from a future attack and will these steps be successful in doing so? Successfully pricing insurance in the long run demands answers to such questions. The experience that a few years have given the companies is important and the estimates now are more accurate than they were five years ago, but more experience is certainly needed before insurers will as comfortably write cyber-risk polices as they write other lines today.

Macroeconomic Consequences of the Cyber-terror Threat

In order to assess the macroeconomic effects of a cyber-attack on computers it may first be useful to examine how computers contribute to economic activity. It is that contribution that is presumed to be at some risk.

Robert Solow, a major contributor to the theory of economic growth, is often quoted for his remark that the effect of computers can be seen everywhere but in the productivity statistics.[56] Through the 1980s and early 1990s, there seemed to be no big payoff from the growing stock of computers. That presented a puzzle to those

---

[56] Robert Solow, "We'd Better Watch Out," *New York Times Book Review*, July 12, 1987, p. 36.

who expected significant returns. But it is now believed that computers have had much to do with an acceleration in productivity growth that began in the mid-1990s.

Consumers have come to expect a rapid rate of innovation in the manufacture of computers. It is also widely expected that the speed and memory capacity of those computers will continue to improve rapidly. Such a rapid rate of technological advance in the development and manufacture of computers was predicted in 1965 by Gordon E. Moore, one of the co-founders of Intel Corporation.[57] Specifically "Moore's Law" predicted that the number of transistors that could be put on a computer chip would double every 18 months. Whether or not that prediction was a self-fulfilling prophecy may be open to question, but the fact is that the pace of technological advance in the manufacture of computers has vindicated Moore's Law over time.

Because of the rapid innovation in the production of computer chips, the prices of computers, as well as other goods related to information processing and communications, sometimes referred to collectively as information technology (IT), have been falling steadily for some time. Between 1959 and 1995, computer prices fell at an average annual rate of nearly 16.9%, and between 1995 and 2002 prices fell at an annual rate of 20.1%.

These price declines reflect substantial improvements in the quality of computers. The Bureau of Labor Statistics (BLS) has developed a procedure for estimating price indexes for goods whose characteristics are changing rapidly. These are referred to as "hedonic" price indexes. Hedonic price indexes attempt to estimate a statistical relationship between prices and a set of characteristics, such as memory and processor speed.

These price indexes are important to the measurement of productivity, because estimating price change is necessary to estimating change in real output and thus productivity. If the rate of price decline in computers is overestimated, then measures of productivity will be overstated. Most studies estimate that, in the late 1990s, prices for personal computers alone fell at an annual rate of somewhere between 30% and 40%.[58]

Rapid declines in computer prices have, not surprisingly, stimulated a surge in investment. Although there are data back to 1959, production of computers was negligible until the 1980s. Thus, even though real output of IT equipment was increasing rapidly, it did not account for a very large share of total output until recently.

Computers have affected growth in productivity in at least two ways. First, there has been rapid productivity growth in the production of computers which, as computers accounted for an increasing share of total production, tended to raise the

---

[57] Gordon E. Moore, Cramming more components onto integrated circuits, *Electronics*, Volume 38, Number 8, April 19, 1965. See also the Intel web site: [http://www.intel.com/research/silicon/mooreslaw.htm].

[58] J. Steven Landefeld and Bruce T. Grimm, "A Note on the Impact of Hedonics and Computers on Real GDP," *Survey of Current Business*, Dec. 2000, pp. 17-22.

overall measure of productivity growth. Second, the sharp drop in computer prices has stimulated increased investment in computers, which has contributed to an increase in the overall amount of capital available to the workforce. This is often referred to as "capital deepening." Increases in the capital stock generally tend to raise worker productivity.

In part because of increased spending on IT equipment, the overall rate of investment spending rose significantly in the 1990s. Prior to the recent acceleration in productivity growth, most analyses found that computers yielded little benefit. One reason is that, until recently, computers accounted for a relatively small share of the total capital stock.[59]

But, that view has now changed. Economists are encouraged that the acceleration in productivity growth of the late 1990s may mean that the economy is on a higher growth path and many believe that computers have had a lot to do with it.

Two recent studies found considerable evidence that the computer, or more generally IT equipment, is behind most of the recent acceleration in productivity growth. There is also evidence of a modest "spillover" into other sectors of the economy. In other words, investment in computers can raise the productivity of the workers who use them, but it may also lead firms to change the way they operate leading to further productivity gains.

The first study, by Oliner and Sichel at the Federal Reserve Board, found that of a 0.9 percentage point increase in the growth rate of total factor productivity from the first half of the 1990s to the second half, all could be accounted for by advances in the production of computers themselves and the also by the use of those computers.[60] Table 6 presents a breakdown of Oliner and Sichel's accounting for productivity growth for selected periods since 1974.

---

[59] Stephen D. Oliner and Daniel E. Sichel, "Computers and Output Growth Revisited: How Big is the Puzzle?" *Brookings Papers on Economic Activity*, 2:1994, pp. 273-334.

[60] Stephen D. Oliner and Daniel E. Sichel, *Information Technology and Productivity: Where Are We Now and Where Are We Going?* Board of Governors of the Federal Reserve System, May 2002, 78 pp.

Table 6. Contributions to Productivity Growth

	1974-1990 (1)	1991-1995 (2)	1996-2001 (3)	change (3) - (2)
Growth rate of labor productivity	**1.36**	**1.54**	**2.43**	**0.89**
Contributions from:				
Capital Deepening	**0.77**	**0.52**	**1.19**	**0.67**
Information technology capital	0.41	0.46	1.02	0.56
Other capital	0.37	0.06	0.17	0.11
Labor quality	**0.22**	**0.45**	**0.25**	**-0.20**
Multi-factor productivity	**0.37**	**0.58**	**0.99**	**0.41**
Semiconductors	0.08	0.13	0.42	0.29
Computer hardware	0.11	0.13	0.19	0.06
Software	0.04	0.09	0.11	0.02
Communication equipment	0.04	0.06	0.05	-0.01
Other nonfarm business	0.11	0.17	0.23	0.06

Source: Oliner and Sichel, op. cit.

Oliner and Sichel found that of an 0.89 percentage point increase in average labor productivity between the early and late 1990s, 0.56 was due to increased investment in IT related capital (an increase from 0.46 to 1.02), and 0.35 was due to increased productivity in the production of IT equipment (an increase from 0.26 to 0.61 in the combined computer and semiconductor sectors). Thus, the contribution of IT equipment to the increase in productivity was greater than the overall increase. Oliner and Sichel also found that labor quality's contribution to productivity growth declined during the 1990s. That is likely related to cyclical factors as the unemployment rate fell and the available pool of skilled workers shrank.

Oliner and Sichel, using an economic model, attempted to assess the implications of recent developments in the technology sector for prospects for continued rapid productivity growth. They conclude that productivity growth is likely to fall somewhere in the range of 2 - 2¾% over the next 10 years.

A second study, by Jorgenson, Ho, and Stiroh, came to similar conclusions.[61] Table 7 presents the results of their analysis.

---

[61] Dale W. Jorgenson, Mun S. Ho, and Kevin J. Stiroh, *Lessons From the U.S. Growth Resurgence*, paper prepared for the First International Conference on the Economic and Social Implications of Information Technology, held at the U.S. Department of Commerce, Washington, D.C., on Jan. 27-28, 2003, 28 pp.

Table 7. Sources of Productivity Growth

	1959-1973 (1)	1973-1995 (2)	1995-2001 (3)	change (3) - (2)
Growth rate of labor productivity	2.63	1.33	2.02	0.69
Contributions from:				
Capital Deepening	1.13	0.80	1.39	0.59
IT Capital Deepening	0.19	0.37	0.85	0.48
Other Capital Deepening	0.95	0.43	0.54	0.11
Labor Quality	0.33	0.27	0.22	-0.05
Total Factor Productivity	1.16	0.26	0.40	0.14
Information Technology	0.09	0.21	0.41	0.20
Non-information Technology	1.07	0.05	-0.01	-0.06

Source: Jorgenson, Ho, and Stiroh.

According to Jorgenson, Ho, and Stiroh's estimates, of a 0.69 percentage point rise in average labor productivity growth during the 1990s, increased investment (capital deepening) accounted for 0.59 percentage point, and improved productivity in the IT sector itself contributed another 0.20 percentage point of the acceleration.

The evidence suggests that increased productivity in the sector producing IT equipment has had a modest direct effect on total factor productivity. By far the more important factor has been the declining price of IT equipment stimulating a surge in investment and increasing the size of the capital stock.

Remember that total factor productivity measures changes in output that are not accounted for by changes in economic inputs such as labor and capital. There is no doubt that computers are raising productivity of many firms, but, as long as economic statistics measure them correctly, the increased share of work that computers do will not show up in increased multi-factor productivity because that measure of productivity tracks the increase in output not associated with the increase in investment in computers.[62] It is unclear whether or not computers have had any "spillover" effects on multi-factor productivity beyond their direct contribution to growth in output.

There is some evidence to suggest that those spillover effects – of computers on total factor productivity – are fairly small. In 2000, Jorgenson and Stiroh found that those sectors of the economy that invest most heavily in computers and IT equipment, such as financial services, had among the lowest rates of productivity growth measured.[63]

---

[62] Barry P. Bosworth and Jack E. Triplett, *What's New About the New Economy? IT, Economic Growth and Productivity,* Brookings Institution, December, 2000, 35 pp.

[63] Dale W. Jorgenson and Kevin J. Stiroh, "Raising the Speed Limit: U.S. Economic Growth (continued...)

Jorgenson, Ho, and Stiroh also estimated projections of growth in average labor productivity. They projected in 2003 that productivity growth would range between 1.14% and 2.38% over the following decade, with a base case of 1.78%, just below the 1995 - 2001 rate of growth.

In another study, Robert Gordon found that most of the acceleration in labor productivity was attributable to capital deepening and faster productivity growth in the production of computers and IT equipment.[64] Of the roughly 0.2 percentage point increase in total factor productivity, most was accounted for by faster productivity growth in the manufacture of durable goods. That suggests that any spillover effects of computers on the overall economy were limited.

It seems evident that, at least in the recent past, computers and other IT equipment have made a significant contribution to the production of goods and services. But those investments may also have introduced new vulnerabilities. Because many of the computer systems are interconnected they may be subject to attacks designed to interfere with their operations.

In the face of uncertainty about the risk and the potential cost of threats to computer operations and security, firms must allocate some resources to the protection of their computer networks and databases. The result is a one-time reduction in the productivity for those firms. Because of the increased need for computer security, there is an increase in the inputs to the production of goods and services without any corresponding increase in the output of those firms. Productivity is a ratio of the output of a firm to the inputs used in the goods produced by that firm. Any increase in inputs that do not contribute to output will reduce measured productivity. In the case of a one-time increase in the cost of computer security there will be a one-time drop in the level of productivity. Firms may also direct IT employees to spend more time on computer security problems and less time enhancing and developing new customer services. Whether or not the increased need for computer security has any long-term effects on productivity growth may depend on improving productivity in the provision of computer security. Unless there is some increase in risk, or unless firms reassess their perception of the potential threat, much of the effect of increased computer security costs on productivity has already happened.

Estimates of the magnitude of the effect on productivity of the increased cost of computer security are hard to come by. There are estimates, however, of the overall effect on productivity of the increased spending on homeland security following the September 11 terror attacks. Increasing physical security is likely to be more expensive than increasing computer security because much of the provision of physical security is labor intensive. In an analysis published by the New York Federal Reserve Bank, Hobijn estimated that increased homeland security spending

---

[63] (...continued)
in the Information Age," *Brookings Papers on Economic Activity*, 2000(1), volume 2, pp. 125-212.

[64] Robert J. Gordon, *Technology and Economic Performance in the American Economy*, Working Paper 8771, National Bureau of Economic Research, Feb. 2002,58 pp.

would have only a modest effect on productivity.[65] Hobijn calculated that if homeland security spending were to double, the one-time total drop in the level of productivity would be 1.1%.

If somehow, a cyber-attack were able to disable some or all of the nation's network of computers, what might the macroeconomic effects be? It might help to put things into perspective by examining previous events that have been labeled "disasters," and looking at estimates of the economic costs associated with them.

The Bureau of Economic Analysis (BEA) is the agency responsible for publishing estimates both of national income and also of the capital stock. In order to do that it must also estimate how much of the capital stock is lost due to some catastrophic event above and beyond the depreciation that occurs over the lifetime of any physical asset. Table 8 presents selected BEA estimates of the value of structures and equipment destroyed as the result of various significant events. The value of the loss is expressed as a percentage of gross domestic product (GDP). Also shown is the rate of economic growth in the quarter preceding the event and for the quarter in which the event occurred as well.

It might be unwise to read too much into the differences in economic growth between the quarter prior to and the quarter of the event. However, it may be worth noting that economic growth declined in less than half of the cases shown. It appears that whatever effect these disasters had on the macroeconomy was not significant relative to other factors that influence economic growth.

There is a fundamental difference between a cyber-attack and a conventional physical attack in that a cyber-attack generally disables – rather than destroys – the target of the attack. Because of that difference, direct comparison with previous large-scale disasters may be of limited use. There have been two other events in the recent past that may also serve as bases for comparison. The first was the requirement to upgrade many computers and their software to avoid what was a potentially serious problem related to recognition of the date in the last year of the 20th century. This was generally known as the "Y2K problem." The second recent event was the electrical blackout that affected much of the northeastern United States in August 2003.

The problems associated with Y2K were different from the potential costs of a cyber-attack in that it was known with some degree of certainty that there was a problem and there was a known deadline by which the problem had to be solved. It was similar in the sense that firms had to divert resources in order to fix a problem in the same way that firms must divert resources to protect their computer networks from attack.

---

[65] Bart Hobijn, "What Will Homeland Security Cost?," Federal Reserve Bank of New York *Policy Review*, Nov. 2002, pp. 21-33.

Table 8. Value of Physical Capital Destroyed by Natural Disasters

Event	Location	Year and quarter	Value as a percent of GDP	Annual rate of change in GDP in:	
				Previous quarter	Event quarter
Earthquake	California	1971:I	0.04	-1.9	-0.7
Hurricane Agnes	Middle Atlantic	1972:II	0.55	7.3	9.8
Flood	Mississippi	1973:II	0.16	10.6	4.7
Tornadoes	Alabama, Indiana, Kentucky, Ohio, Tennessee	1974:II	0.05	-3.4	1.2
Flood dam collapse	Idaho	1976:II	0.03	9.3	3.0
Windstorms, flood	Kentucky, Virginia, West Virginia	1977:II	0.07	4.9	8.1
Floods, Tornadoes	Alabama, Mississippi, North Dakota, Arkansas, Texas	1979:II	0.06	0.8	0.4
Hurricanes David and Frederick	Alabama, Mississippi	1979:III	0.10	0.4	2.9
Mudslides	California	1980:I	0.03	1.2	1.3
Riots, Mount St. Helens eruption	Miami (Florida),Oregon, Washington	1980:II	0.04	1.3	-7.8
Hurricane Iwa, Floods	Hawaii, Arkansas, Missouri	1982:IV	0.10	-1.5	0.4
Hurricane Alicia	Texas	1983:III	0.12	9.3	8.1
Hurricanes Elena and Gloria	Atlantic and Gulf Coasts	1985:III	0.08	3.5	6.4
Tropical Storm Juan, Hurricane Kate, Floods	Atlantic and Gulf Coasts	1985:IV	0.08	6.4	3.1
Hurricane Hugo	North and South Carolina	1989:III	0.29	2.6	2.9
Earthquake	Loma Prieta (California)	1989:IV	0.26	2.9	1.0
Fire	Oakland (California)	1991:IV	0.10	1.9	1.9
Hurricane Andrew	Florida, Louisiana	1992:III	1.02	3.9	4.0
Hurricane Iniki	Hawaii	1992:III	0.13	3.9	4.0
Winter Storm	24 Eastern States	1993:I	0.12	4.5	0.5
Floods	9 Midwestern States	1993:III	0.13	2.0	2.1
Earthquake	Northridge (California)	1994:I	1.15	5.5	4.1
Hurricane Opal	10 Southern States	1995:IV	0.13	3.3	3.0

Source: Department of Commerce, Bureau of Economic Analysis.

There was some uncertainty regarding the possible economic effects of not fixing the Y2K glitch, but because the problem was widely recognized well in advance and there were clear incentives (including regulatory mandates for some) to fix it ahead of time, the year change in fact presented no indication of difficulty.

Total spending, private and public, to upgrade computers and software to avoid the Y2K problem has been estimated at about $100 billion.[66] In some cases, software upgrades that solved the problem might have taken place anyway, since the useful lifetime of software tends to be much shorter than the useful lifetime of most physical assets. There also may have been a slight offsetting boost to productivity because of Y2K preparations. Some software and hardware upgrades that had not been scheduled to take place prior to the date change were sped up along with any addition to productivity they may have contributed.

The electrical blackout of August 2003, may also serve as a case for comparison. Estimates of the cost of the blackout range from $6 to $10 billion for the entire U.S. economy.[67] That accounted for 0.1% of GDP. The power failure imposed costs on both households and businesses. Production was disrupted, affecting earnings and profits, food stocks spoiled because of lack of refrigeration, and government costs rose because of the increased demand for police and other emergency services. In some cases production may have simply been delayed in which case losses may not have been permanent; but in other cases businesses may not have been able to make up the loss by shifting production.

The determinants of the cost of the power outage were principally the size of the area affected and the duration of the blackout. Costs may have been less than they otherwise would have been because power was lost late in the afternoon and began to be restored the following morning.

Of all the cases cited, the northeast power failure may be the most relevant to a consideration of the potential costs of a cyber-attack. In the case of the power failure, there was little, if any, destruction of physical capital. The cost of the outage was primarily determined by its size and duration. Those two factors would likely also determine the economic cost of a cyber-attack.[68]

Any estimate of the potential economic cost of a cyber-attack must ultimately be speculative. Computers and other information processing equipment that might be vulnerable to attack make a direct contribution to the production of goods and services. But it is unclear how much other factors of production, both labor and capital, are dependent on computers. It seems within the realm of possibility that the effect of an attack on computers and their networks could have an effect on output

---

[66] U.S. Department of Commerce, Economics and Statistics Administration, "The Economics of Y2K and the Impact on the United States," Nov. 1999, 25 pp.

[67] See, for example: Anderson Economic Group, "Northeast Blackout Likely to Reduce US Earnings by $6.4 Billion," Aug. 19, 2003, 8 pp.; The Brattle Group, "Economic Cost of the August 14th 2003 Northeast Power Outage: Preliminary Estimate," Aug. 18, 2003, 4 pp.; ICF Consulting, "The Economic Cost of the Blackout," 3 pp.

[68] This presumes that any data and software have been backed up and stored in such a way that they can not be corrupted, and that they can be restored once the attack has subsided.

much larger than that amount that is accounted for by their direct contribution. Electric power supplies might be affected. Banks might be unable to transfer funds. Electronic payment for goods and services might be interrupted. Market transactions might be limited to whatever currency is in circulation. A significant proportion, if not all, of total production might be interrupted. For all of these things to occur simultaneously would presumably require an extremely sophisticated attack that was completely successful. While the probability of such an event may be extremely low, it still gives a basis for an upper limit to any estimate of the economic damage that might be done.

If all economic activity were to be temporarily interrupted by a cyber-attack, the only consideration in estimating the cost would be the duration of the event. The share of GDP produced on a given day is about 0.3% of the total for the entire year. Some of the production that might be interrupted is unlikely to be a permanent loss, but would simply be deferred until the effects of the attack dissipated. Since a considerable, if unknown, share of output is not dependent on computers, the final cost would be less than that.

Historically, total annual production of goods and services has averaged roughly one-third of the value of the total stock of physical capital. As of 2001, computer equipment and software accounted for roughly 18% of the total capital stock. If equipment and software are assumed to contribute to output in the same way as other forms of capital, their direct contribution would account for about 18% of total annual production.[69] If that share of output were interrupted for a single day it would amount to about 0.05% of total annual GDP.

As long as any cyber-attack is less than comprehensive and short-lived it is likely that any macroeconomic consequences will be fairly small. But, whatever the scope of the attack, the ability to recover quickly is important, since the length of time computers are affected is an important determinant of the costs. It may be almost as important for firms to address their abilities to restore operations as it is to work to insulate themselves from any potential attack.

---

[69] Their indirect contribution is higher to the extent that other sectors, such as communication and transportation, rely upon them. Setting a figure on this indirect contribution is impossible.

Conclusion and Policy Options

This report has described the difficulties that attend the measurement and quantification of cyber-risk. There is no question that our present level of knowledge is below what we would like it to be. By briefly setting out the chief obstacles to progress, and the market forces that are driving efforts to improve cyber-risk management, some conclusions about the avenues available to policy makers can be drawn.

The first major obstacle is the lack of data on the frequency and severity of cyber-attacks. Organizations – particularly private businesses – have strong incentives not to share information about attacks. Several government agencies are planning or conducting survey research on a much greater scale than has been done before; the results, together with other government-sponsored efforts to increase information sharing, may in time lead to significant improvements in our ability to assess cyber-risk. If incentives to conceal information remain strong,[70] however, some form of mandatory reporting regime might be considered. A model could be the public health system, where the benefits of a central data base on cases of certain illnesses outweigh an individual's right to privacy.

The other chief obstacle is the inherent difficulty in measuring costs that may be intangible and subject to innumerable contingencies. Current research focuses on how to improve quantification of risk and costs in the face of this complexity. "[I]t is too hard to solve the fully general security problem. Therefore, we must simplify, we must model."[71] Modeling involves a trade-off: the simpler the model, the easier to use, but if a model is too simple, it may fail to capture cyber-risk in its entirety. On the other hand, if a model is elaborated to take into account more and more possible attack scenarios, it may become so complex that the cost of measurement itself becomes material to the risk management calculation, particularly for small firms and organizations. At the present stage of knowledge, we cannot identify any one best cyber-risk model that all firms and organizations could usefully adopt. There may never be such a one-size-fits-all procedure.

There are three major market forces at work that will lead to improvements in cyber-risk management: competition, liability, and insurance. What might policy do to encourage these forces, or at least not to interfere with them?

Firms that best manage cyber-risk will be rewarded by a competitive market. This simple statement implies that it may be premature for policy makers to attempt to move forward with a general standard for risk management. In addition to the information on security research published in journals and conferences, we can be sure that much of the cutting-edge work in the field is being done out of the public eye, behind the corporate proprietary veil. It may be useful for public and private groups to put forward sets of guidelines and best practices, but only to the extent that these are seen as minimum requirements, not complete and sufficient responses to

---

[70] And the recent experience of the Bureau of the Census suggests that they do (see p. 14).

[71] Daniel Geer, Jr., "Making Choices to Show ROI," *Secure Business Quarterly*, v.1, 4th quarter 2001, p. 3.

cyber-risk. Deciding that today's methods are good enough may discourage future research.

The second market force is liability. The prospect of being sued for damages when confidential information is stolen or destroyed is a major incentive for firms to improve information security. It is also, however, a major disincentive for sharing information about cyber-attacks. Some may suggest that limits or caps on liability related to cyber-security breaches would make firms less reluctant to disclose incidents. In theory, lower liability would also reduce the incentive to invest in security, but, in practice, since liability is only one of many costs that influence risk management decisions, this effect might be very slight.

Finally, market forces – in the form of profit opportunities – are driving the development of cyber-risk insurance. A thriving insurance market would greatly reduce the costs associated with the inability to quantify risk. With insurance, firms would not have to measure potential risks of cyber-attacks themselves, any more than homeowners have to calculate the exact probability that their houses will burn down. Significant economic efficiencies will be obtained as the risk assessment function is shifted from millions of individual organizations and firms to insurers, who specialize in pricing risk. Growth of cyber-risk insurance is hindered primarily by a lack of reliable actuarial data related to the incidence and costs of information security breaches; enhanced collection of such figures would probably be the most important contribution that policy can make.

Appendix A. An Overview of Cyber-Risk Management in a Fortune 500 Manufacturing Company

Information Protection Management Guidelines

Background:

The Information Protection Management Guidelines (IPMG) were developed by a non-profit organization in collaboration with IT managers from all divisions, and approved by the IT Leadership Team in 2001. The IPMG provides standards and guidance for all business units to utilize good information protection practices to ensure the company's confidential and proprietary information, in all of its forms, is protected.

Highlights of the IPMG:

Risk-based Approach to Information Security

The IPMG's underlying principle is to require business units to assess the risk to information from the perspective of impact to the company and the likelihood of an attack against that information. The areas of exposure are unauthorized disclosure, modification, and loss of availability of information. By classifying information into risk levels, business units will ensure that cost of protection is justified by the severity and likelihood of exposure.

Risk Levels

The IPMG sets risk levels at four levels:

Level 3	Irreparable Harm to the Company, Very likely target
Level 2	Significant Harm, Possible target
Level 1	Moderate Harm, Unlikely target
Level 0	No Harm, Not a target

Most of the company's information falls into Level 0 and Level 1. Only a small percentage of information falls into the highest risk level of 3.

Information Security Officers (ISOs)

The IPMG requires that business units appoint ISOs to implement the information protection guidelines. Corporate Security provides a training class on information protection, including the methodology for determining risk levels and developing a cost effective Information Protection Plan (IPP). Currently, there are approximately 400 trained ISOs throughout the Company.

Information Protection Control Objectives (Controls Matrix)

The IPMG contains a detailed matrix of approximately 200 information security controls, based on Risk Level, which provides specific guidance to ISOs and IT professionals for proper information protection. These controls are consistent with best practice and internationally recognized information security standards (ISO standard 17799). The controls include detailed standards in areas of password policy, auditing and logging, authentication, confidentiality, network security, third party and remote access, standards for vendors, temps, and consultants, and other relevant areas.

Information Protection Plans

ISOs are responsible for developing IPPs for their business units, and implementation of the applicable controls. Global Security has developed a web based software utility to assist ISOs in plan development, including the automated selection of applicable controls.

Compliance

Corporate Internal Audit (CIT) is responsible for auditing business unit compliance to the IPMG.

CIT and IT Groups

CIT is responsible for providing the technical infrastructure and IT security services to secure the enterprise and assist divisional IT groups in meeting the control objectives. Thus, IT groups are able to select which security services are required to meet the requirements of their IPP.

Appendix B. Cyber-Risk Management in the Financial Services Sector

Recovery modes to mitigate financial market disasters, including such special cases as cyber-attacks, have been developed and tested from within and without the financial providers' networks. Financial responsibility requires the financial institutions so important in supporting and maintaining domestic and international commerce to take steps to safeguard their ability to carry out basic functions. The backbone of the financial economy—the payment system—comes through banks, only two of which form the entire and vital U.S. government securities clearing and settlement market. Other crucial intermediation functions come through a variety of other financial companies, including brokers, exchanges, other secondary market facilities, and insurance companies. Thus, many regulators and trade associations are involved. The combinations of public and private initiatives have largely resulted in qualitative prescriptions to date; no government regulation numerically dictates how much information security spending a financial institution, or indeed any company, must undertake.

Financial institutions, not only banks and other depositories, but also securities dealers, insurers, and investment companies, are collectively considered a critical infrastructure element for the U.S. economy.[72] They also rely heavily on information technology, both making them particularly vulnerable to cyberattack and amplifying the danger from such an attack. Long before 9/11/01, analysts identified financial sector system vulnerabilities as elements of national economic security in the work of the President's Commission on Critical Infrastructure Protection in 1996 and 1997.[73] America has grown far beyond a bank-centered financial economy started with bank notes; financial value has largely become resident on computers as data rather than physical means of payment.

Financial institutions face two categories of emergencies that could impair their functioning. The first is directly financial: danger of a sudden drop in the value of financial assets, whether originating domestically or elsewhere in the world, such that a global financial crisis might follow. The second is operational: failure of physical support structures that underlie the financial system. Either, whether from natural causes or human malice, could disrupt the nation's ability to supply goods and services and alter the behavior of individuals in fear of the disruption (or fear of greater disruption). This could reduce the pace of economic activity, or at an extreme, cause an actual contraction of economic activity. Financial regulators generally address the former set of problems through deposit

---

[72] See, for example, Homeland Security Presidential Directive 7, issued December 17, 2003, at [http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html], visited Mar. 17 2003.

[73] "The President's Commission on Critical Infrastructure Protection," on web site [http://www.ciao.gov/resource/commission.html]; and, "Banking and Finance," on web site [http://www.ciao.gov/resource/pccip/ac_bank.pdf], visited Apr. 15, 2003.

insurance and other sources of liquidity to distressed institutions, safety and soundness regulation, and direct intervention. They address the latter set of problems through remediation (as with the Y2K problem), redundancy, and other physical security protocols.

Financial firms' regulators, separately and collectively, have issued regulations for redundancy and security in physical systems and financial systems. They have long required banking institutions to consider operating (security) risks such as embezzlement, fire, flood, robbery, etc., to which they have added physical-and cyber-terrorism in specific terms during recent years. Many of the protocols address problems arising from any kind of computer/electrical shutdown, while others necessarily address only one adversity such as denial-of-service attacks. By necessity, many protocols remain confidential, as both public-sector and private-sector participants realize that concealed defenses, or even the suggestion of such defenses, act to deter cyberattacks.

Regulators, especially the Fed, have set out best practice guidelines. These steps include business information technology protocols, physical security protocols, and plans for continuity of markets and participants considered critical for the nation's transactions. The "Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System,"[74] issued by the Fed, the OCC, and the SEC, is aimed at assuring the survivability of financial businesses. Controversies have arisen; e.g., some insurers believe that federal regulators have no authority to require them to take such steps, and some in New York are concerned that the area will lose jobs as facilities are necessarily dispersed. Costs of undertaking security measures also remain of concern. Further governmental and public-private initiatives have sought to strengthen the resiliency of the financial system's computers in view of increasing cyberattacks.

Role of Department of Homeland Security.

The Department of Homeland Security (DHS) has jurisdiction over functions previously assigned to many agencies with respect to certain communications, transportation, and computer ("cyber") security. These are essential parts of the physical infrastructure upon which the financial system relies as a user. They are also parts of the electronic infrastructure of information storage, retrieval, and transmission. The heart of financial services is information that providers transform into useful forms, such as account balances at banks, securities price quotations, executions of purchase and sales of financial assets, and payments on contractual obligations such as loans.

Although networks of communication are vital to their work, financial services companies do not generally maintain communications and transportation networks, nor design software or manufacture hardware and carriage devices such as airplanes and trucks. Security of communication thus resides with sectors

---

[74] *Federal Register*, vol. 68, no. 70, April 11, 2003, pp. 17809-17814.

covered by DHS.[75] Financial institutions and their regulators operate in a different environment than nonfinancial ones: they have been developing appropriate (sometimes different) security protocols within existing frameworks. DHS interacts with the Treasury Department, which has taken the lead role for the overall defense of finance against cyberattacks. The Treasury has recently reached agreement with DHS to assign an expert in financial services matters from Treasury to Homeland Security. Eventually, experts from other financial regulators will be rotated into that new position.[76]

Safety and Continuity in Recent Experience.

Y2K Threat. The widely anticipated Y2K "millennium bug" was a software programming problem that could have caused failures in the infrastructure upon which the system relies. Public and private groups spent much effort to prevent widely feared collapse of financial capabilities on January 1, 2000; they succeeded. Y2K came and went without serious incident in 2000, but the systematic backups and safeguards provided against it proved invaluable when the unthinkable happened the next year.

2001. With the September 2001 destruction of the World Trade Center, both potential problems—financial loss of asset values, and operational interruption—occurred simultaneously.

The financial side of the response worked well, as the Fed provided the necessary liquidity to prevent panic.[77] The SEC issued emergency rules encouraging buying in the stock market once it reopened. Trading recommenced rapidly, as the U.S. Treasury security market opened on September 13, and the equities market was in full operation by September 17.

Physical infrastructure recoveries took a few days of heroic efforts (e.g., running new connections into Manhattan). Off-site record keeping and backup facilities, sharing of working space with displaced competitors, and increasing reliance on electronic tracing and communications systems by institutions outside the attack area allowed for resumption of near-normal operations quickly. Much of the off-site infrastructure and response plans had already been developed in the aftermath of the 1993 bombing at the World Trade Center. Physical and virtual destruction of the heart of the nation's financial markets did not stop their workings for more than a few days. Nonetheless, regulators and industry groups made it known that financial firms would need new contingency plans and stress tests to protect against extreme situations in the future.

---

[75] See "Administering the New Department of Homeland Security," on web site [http://www.congress.gov/erp/legissues/html/isdhs2.html], visited April 15, 2003.

[76] "Treasury Introduces Upgrades Designed To Help Safeguard Financial Service System," *BNA's Banking Report*, Dec. 8, 2003, p. 836.

[77] "Economic Repercussions: Overview," by Gail Makinen. In the CRS *Electronic Briefing Book on Terrorism*, at web site [http://www.congress.gov/brbk/html/ebter110.html], visited April 15, 2003.

Blackout of 2003. It seems emergency response measures helped reduce the financial market damages from the massive Aug. 14 power blackout in the northeastern United States and Canada. The Treasury Department received no reports of major disruptions or losses of financial data, in large part because of steps taken to make systems resilient and redundant. Despite glitches, the major markets, in stocks, options, commodities, futures, and bonds, were soon open. Banks closed affected offices, but otherwise, the banking system stayed open. The Fed's payments and emergency lending to banks systems operated well. Banks borrowed $785 million from the Fed after the blackout, the most since $11.7 billion in the week after Sept. 11, 2001. When it was determined, contrary to initial fears, that terrorists had not caused the blackout the stress on the financial economy was greatly reduced.[78] Such initial fears may have been raised by recent press reports of the increasing frequency and severity of cyberattacks directed against financial institutions. A paging and alert system set up after 9/11 by the Financial Services Roundtable (a group of major financial providers) and its technology arm, called BITS, aided the rebound from the computer shutdown due to the blackout. [79]

---

[78] "Measures Prompted by Sept. 11 Helped Banks Weather Electrical Outage, Snow Says," *BNA's Banking Report*, August 25, 2003, p.254; Todd Davenport, "In Brief: Outage Sparked $785M of Fed Lending," *American Banker Online*, Aug. 22, 2003; and Rob Blackwell, "Backup Site Questions, Utility Loan Prospects," *American Banker Online.,* Aug. 18, 2003.

[79] Blackwell, "Backup Site Questions."