NIST Advanced Manufacturing Series 100-32

Cybercrime Losses

An Examination of U.S. Manufacturing and the Total Economy

Douglas Thomas, Economist

This publication is available free of charge from:
https://doi.org/10.6028/NIST.AMS.100-32

National Institute of
Standards and Technology
U.S. Department of Commerce

NIST Advanced Manufacturing Series 100-32

Cybercrime Losses: An Examination of U.S. Manufacturing and the Total Economy

Douglas Thomas, Economist
Applied Economics Office
Engineering Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.AMS.100-32

April 2020

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Undersecretary of Commerce for Standards and Technology

National Institute of Standards and Technology Advanced Manufacturing Series 100-32
Natl. Inst. Stand. Technol. Adv. Man. Ser. 100-32, 50 pages (April 2020)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.AMS.100-32

Abstract

Cybercrime puts America's competitive edge and economic future at risk; however, there is some debate as to the extent that this activity is impacting economic activity. This report examines a selection of the current estimates of U.S. losses due to cybercrime. Many have questioned the validity of estimates of cybercrime losses, concluding that "they are so compromised and biased that no faith whatever can be placed in their findings" (Florencio and Herley 2016). Some approximations are potentially underestimating/overestimating the losses due to under sampling. Others do not report out data that lend themselves to estimating national aggregated losses. It is difficult to substantiate sampling issues, as the methods used are often only partially documented, a problem in and of itself; however, most acknowledge that there are serious data limitations. To address the issues and challenges raised, this report does the following:

- Identifies and utilizes data with a large sample size
- Utilizes data that fully discloses methods and results
- Utilizes data that is collected and reported by an organization experienced in data collection and reporting
- Estimates a range of losses by making assumptions that bias the upper estimate upward and the lower estimate downward
- Stratifies loss estimates by industry groupings
- Examines national losses as opposed to global losses

The most statistically reliable data identified for measuring U.S. cybercrime losses is from a survey of 36 000 businesses with 8079 responses conducted by the Bureau of Justice Statistics. This is the largest sample size that could be identified that disclosed methods and results. Using this data combined with methods of uncertainty analysis, upper and lower boundary estimates were made. These approximations are consistent with the hypothesis that current widely cited values might actually underestimate the losses due to cybercrime. The 2016 losses are estimated to be between $167.9 billion and $770.0 billion or between 0.9 % and 4.1 % of U.S. GDP, a substantial amount of loss that is based on business' estimates of their losses. For manufacturing, the loss is between $8.3 billion and $36.3 billion or 0.4 % and 1.7 % of manufacturing value added. The low estimate is calculated making the assumption that those who did not respond to the Bureau of Justice Statistics survey did not experience any losses, which is an unlikely scenario that biases it downward. Although it is possible that the true loss approaches the upper limit, the results from a Monte Carlo simulation put 90 % of the simulated values below $473 billion or 2.5 % of GDP. The high estimate assumes the average loss per company of the respondents equals the average loss per company in the U.S.

Key words

cybercrime; economics; loss; manufacturing; GDP; gross domestic product; value added; crime

Table of Contents

List of Tables

List of Figures

1. Executive Summary

Cybercrime[1] puts America's competitive edge and economic future at risk. In some ways, like companies, countries compete, economically, based on two primary methods: cost and differentiation. The U.S. tends to produce high-cost high-quality goods, making it more of a differentiator than a cost competitor. For differentiators, protection of intellectual property is critical; otherwise, competitors can simply commandeer those things that differentiate one competitor from another. Moreover, cybercrime puts U.S. intellectual property at risk.

There is some debate as to the extent cybercrime affects the economy. On one hand, cybercrime is seen by some as "the greatest transfer of wealth in human history;" however, others claim it is a "rounding error in a fourteen trillion-dollar economy" (Center for Strategic and International Studies 2013). There are a great deal of individuals that are skeptical of high estimates of cybercrime costs and there are often assumptions their costs do not exceed that of other types of crime (Hyman 2013). These assumptions and views may not be well supported, as the current data is not reliable. Nearly every estimate acknowledges the great uncertainty associated with their numbers. For instance, McAfee states that, "estimates of the cost of cybercrime still show significant variation, from tens of billions to a trillion dollars or more. This reflects the absence of data and differing methodologies" (McAfee 2018).

The cyber world is relatively new and, unlike other types of assets, cyber assets are potentially accessible to criminals in far off locations. This distance provides the criminal with significant protections from getting caught; thus, the risks are low, and the payoff is high. There is little justification in assuming much about the national losses due to crime in this new world. Most of the publications on cybercrime costs are non-technical in nature and provide few details on the methods or data used. There is a need for more rigorous data collection and methods documentation. The current data situation is dismally inadequate for making even general estimates of the losses due to cybercrime (Eling and Schnell 2016). Despite this situation, this report is able to provide lower and upper bound limit estimates. Due to the data limitations, though, these estimates have a wide range.

The total activities and assets at-risk due to cybercrime in 2017 for the U.S. amounts to $11.9 trillion, as reported by the Bureau of Economic Analysis (2020). This includes the 2017 digital economy ($1.4 trillion) and assets that could potentially be digitally connected ($10.5 trillion), as estimated for 2018. The manufacturing industry's share of at-risk activities and assets is $4.4 trillion. Its share of the digital economy is $129.8 billion. Its share of assets is $4.3 trillion. Note that this is an upper limit, as only some portion of the assets are digitally connected.

A focus of this report is on the effect of cybercrime on U.S. manufacturing; however, given the data challenges present, it is necessary to examine cybercrime's effect on all

[1] For this report, cybercrime includes security incidents in which a computer was used as the means of committing a crime. This includes computer viruses, denial of service, vandalism/sabotage, embezzlement, fraud, theft of intellectual property, and theft of personal/financial data. This report focuses on cybercrime against companies as opposed to those targeting individuals.

industries. Therefore, this report examines a selection of the current estimates of U.S. losses due to cybercrime and concludes that some approximations may actually be underestimating the losses, possibly due to under sampling. It is difficult to substantiate this conclusion, as the methods for estimation are often only partially documented, a problem in and of itself; however, most acknowledge that there are serious data limitations. Losses due to criminal activity commonly follow a lognormal distribution and evidence suggests that cybercrime follows this trend. This issue often means that a large sample is required to generate a representative estimate. To address the issues and challenges of estimation, this report does the following:

- Identifies and utilizes data with a large sample size
- Utilizes data that fully discloses methods and results
- Utilizes data that is collected and reported by an organization experienced in data collection
- Examines uncertainty using Monte Carlo analysis
- Estimates a range of losses by making assumptions that bias the upper boundary upward and the lower boundary downward
- Stratifies loss estimates by industry
- Examines national losses as opposed to examining global losses, which would, likely, pose additional challenges

The most statistically reliable data identified is from a survey of 36 000 businesses with 8079 responses conducted by the Bureau of Justice Statistics. This is, by far, the largest sample that could be identified for examining aggregated U.S. cybercrime losses. Using this data combined with methods of uncertainty analysis, upper and lower boundary estimates were made. These estimates show losses in 2016 to be between 0.9 % and 4.1 % of total U.S. GDP, a substantial amount of loss that is based on what businesses believe they lost. For manufacturing (North American Industry Classification System (NAICS) code 31-33), the loss is between $8.3 billion and $36.3 billion or 0.4 % and 1.7 % of manufacturing value added. While most other estimates tend not to present technical details of data collection and analysis, this estimate is based on public data where the survey instrument is disclosed, as are other details about the data. Further, the method for estimation is described in detail in this report. The estimates made here exceed those of many others, which tend to have limited disclosure of methods/data and tend not to publish uncertainty analyses. Since the data from the Bureau of Justice Statistics is from 2005, these estimates are likely low, as the digital economy grew 129 % between 2005 and 2016 (Bureau of Economic Analysis 2020) and the number of businesses, which is used for estimation, is lower in 2016, according to the Annual Survey of Entrepreneurs..

The most widely cited estimate of losses for the U.S., which is from McAfee (2014), is that cybercrime amounts to 0.64 % of U.S. GDP (i.e., $107.4 billion); however, the data/methods used are only generally described. In 2016, 0.64 % of GDP equated to $119.8 billion. The low estimate of $167.9 billion (i.e., 0.9 % of GDP), presented above, is calculated making the assumption that those who did not respond to the Bureau of Justice Statistics survey did not experience any losses. This amounted to 77 % of the

36 000 businesses surveyed being presumed as having no loss; thus, the true loss is likely higher than the low estimate. Despite making an assumption resulting in a downward biased lower boundary, it is still 40 % higher than the McAfee estimate, which is acknowledged by McAfee as having a great level of uncertainty. The high estimate of $770.0 billion, likely, suffers from selection bias and other issues, making it unlikely that the true value is higher than this estimate. Although it is possible that the true loss approaches this upper limit, the results from a Monte Carlo simulation put 90 % of the values below $473 billion (i.e., 2.5 % of total GDP). It is important to note that if the Bureau of Justice Statistics data is representative, that is, if the average losses per company of the respondents equals the actual average U.S. losses per company, then the losses approach the high estimate of $770 billion.

2. Introduction

2.1. Background

Cybercrime is anticipated to grow as more individuals and companies conduct business online. It affects manufacturers along with other types of businesses and their supply chains. Unfortunately, there is limited data on cybercrime. For instance, the U.S. National Incident-Based Reporting System, an incident-based reporting system used by U.S. law enforcement, does not have a category that covers cybercrime. In 2001, the U.S. Bureau of Justice Statistics piloted a survey on cybercrime, which was sent out again in 2005; however, this program has not continued since that time. Other data collection efforts might cover some portion of cybercrime (e.g., identity theft data presented in the National Crime Victimization Survey); however, these datasets are far from comprehensive and often do not differentiate when a crime was committed electronically versus other means.

There are, increasingly, more digital assets being created, and physical assets are frequently vulnerable to cybercrime. As illustrated in Figure 3.1, between 1997 and 2017, the U.S. digital economy grew at a compound annual rate of 9.9 %; meanwhile the total economy only grew at a 2.3 % rate annually. Without information on the magnitude of cybercrime, it is not clear to what extent investments should be made in risk mitigation. In the UK, for instance, 41 % of manufacturers do not believe they have access to sufficient information to confidently assess their risk, 45 % are not confident that they are prepared, and 12 % have no process measures in place to mitigate against a threat (MAKE UK 2018).

Cybercrime puts America's competitive edge and economic future at risk. The Allianz risk barometer ranks cyber incidents as the primary risk facing businesses out of ten factors, determined by 2718 survey respondents (Allianz 2020). Similarly, PWC identified cyber threats as the primary concern regarding organization growth in the US, as identified by 2700 respondents to their annual Global CEO Survey (PWC 2020). Similar to companies, countries compete, economically, based on two primary methods: cost and differentiation. The U.S. tends to produce high-cost high-quality goods, making it more of a differentiator than a cost competitor. For differentiators, protection of intellectual property is critical; otherwise, competitors can simply commandeer those things that differentiate one competitor from another.

2.2. Scope

This report reviews estimates of U.S. cybercrime losses and generates estimates using a selection of methods. Much of the data and information on cybercrime is described in terms of attacks per year or percent change in attacks (Jardine 2015); however, these numbers do not reveal the success rate and subsequent losses. Therefore, they fail to gauge the scale of the risks that are present.

2.3. Approach

The approach presented in this report utilizes data from a 2005 Bureau of Justice Statistics survey along with other publicly available data on the U.S. economy. Since it is believed that cybercrime has increased over time, this is, likely, to be an underestimate given the publication date of the survey data. Boundary estimates are made where the upper boundary is biased upward, and the lower boundary is biased downward. A probabilistic sensitivity analysis using Monte Carlo analysis was conducted to examine the impact of fluctuating different variables. This technique is based on works by McKay, Conover, and Beckman (1979) and by Harris (1984) that involves a method of model sampling.

There are two economic aspects of cybercrime that are discussed below. The first is the value of assets and activities that are at risk. Understanding this value provides some understanding of the upper limit to the damage that cybercrime can inflict on the U.S. economy. The second issue is in regard to the losses that result from cybercrime.

3. Assets and Activities at Risk

One component of understanding the costs and risks that cybercrime poses, is to measure the assets and activities that are at risk. There are assets and activities that are directly and indirectly at risk. Those that are directly at risk include the digital economy while those that are indirectly at risk are those that are connected in some way to the cyber world. For instance, a piece of machinery or automobile that is connected digitally.

The U.S. digital economy was estimated to be $1.4 trillion in 2017, amounting to 6.9 % of total GDP (measured in current dollars) with digital goods being $124.1 billion and digital services being $1227.2 billion (Bureau of Economic Analysis 2020).[2] These are the value of activities that are directly at-risk from cybercrime. As illustrated in Figure 3.1, between 1997 and 2017, the U.S. digital economy grew at a compound annual rate of 9.9 % while the total economy only grew at a 2.3 % rate annually.

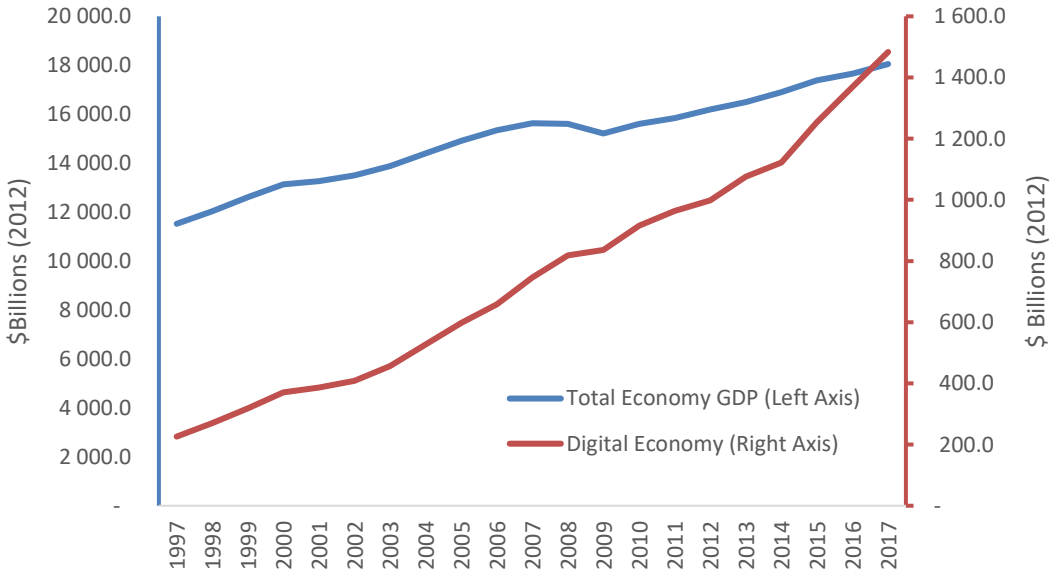

Figure 3.1: U.S. Real Value Added for the Digital Economy

Source: Bureau of Economic Analysis. (2019). Digital Economy. https://www.bea.gov/data/special-topics/digital-economy

The manufacturing industry's (i.e., NAICS 31-33) share of the digital economy is 9.6 % or $129.8 billion, and, as illustrated in Figure 3.2, had a compound annual growth rate of 18.0 % between 1997 and 2017. Industries that handle manufactured goods, including wholesale/retail trade, transportation, and warehousing, account for another $120.7 billion. These two together amount to 18.5 % of the digital economy.

[2] NOTE: "BEA includes in its definition of the digital economy three major types of goods and services: the digital-enabling infrastructure needed for an interconnected computer network to exist and operate; the e-commerce transactions that take place using that system; and digital media, which is the content that digital economy users create and access. Because of the limitations of available data, BEA's initial estimates include only goods and services that are "primarily digital." This means that some components of the digital economy, like peer-to-peer (P2P) e-commerce, also known as the sharing economy, are excluded from the initial estimates" https://www.bea.gov/data/special-topics/digital-economy

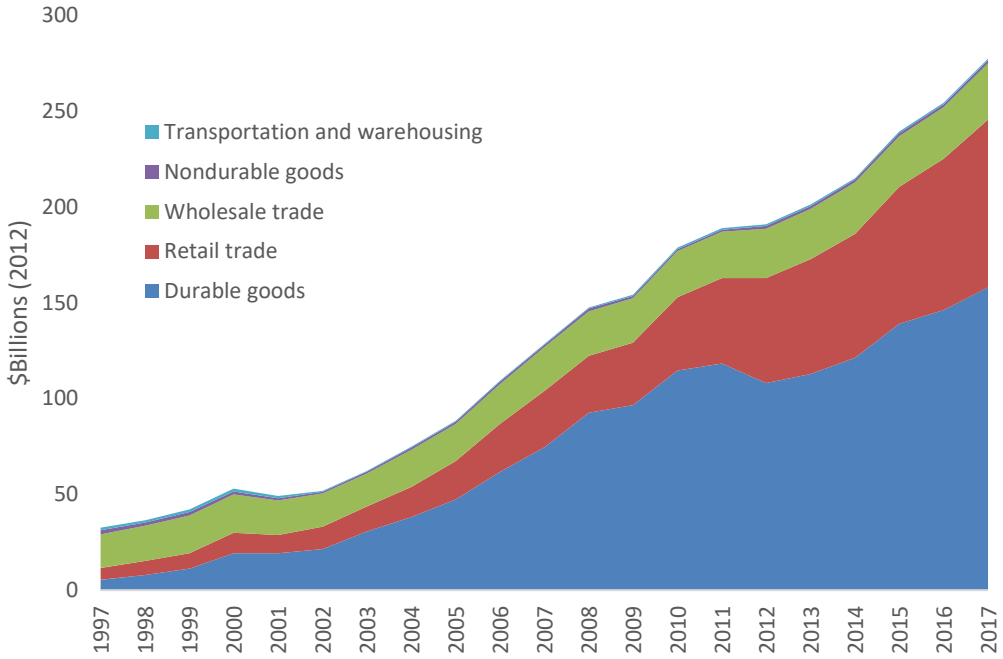

Figure 3.2: Digital Economy - Goods Handling Sectors (2017)

Source: Bureau of Economic Analysis. (2019). Fixed Assets. https://apps.bea.gov/iTable/index_FA.cfm

In addition to economic activities at-risk, there are assets that are at risk and the loss of these assets can have cascading effects on other activities. The 2018 current-cost net stock of U.S. private fixed assets that could be construed as being vulnerable to cyber-attack is valued at $10.5 trillion, as reported by the Bureau of Economic Analysis (2019). To put this in perspective, the 2018 U.S. gross domestic product was $20.6 trillion. The assets at-risk include the total of all information processing equipment ($1.6 trillion), industrial equipment ($2.2 trillion), transportation equipment ($1.6 trillion), other equipment ($1.6 trillion), and intellectual property products ($3.4 trillion). This estimate is an upper limit, as only a selection of these are vulnerable. For instance, not all equipment or vehicles are digitally connected. Also, a great deal of intellectual property products are not concealed. For instance, patented/copyrighted work and trademarked logos have intellectual property value, but are not concealed knowledge that could be stolen. Although they can be counterfeited, they are not vulnerable due to potential cyber-attacks. The share of the at-risk assets, estimated by the Bureau of Economic Analysis (2019), that we identify as relevant to the manufacturing industry are valued at $4.3 trillion and include industrial equipment ($2.2 trillion), manufacturing industry research/development ($1.4 trillion), and trucks/buses/trailers ($699.8 trillion).

The total at-risk activities and assets for the U.S. economy (i.e., the sum of the digital economy and assets) amounts to $11.9 trillion. For manufacturing, the value is $4.4 trillion. Note that, as previously discussed, this is an upper limit, as only some portion of the assets are at risk.

4. Losses

There is no systematic collection of public data on the cybercrime that puts them at risk despite over a trillion dollars of annual value added at-risk and trillions more in assets. With limited data on the incidents, measuring the losses due to cybercrime is challenging. Many losses go unreported. For instance, Google was hacked in 2010 along with 34 other Fortune 500 companies. Much of the information on this incident was only revealed due to documents posted on Wikileaks (Intel Security 2014). Further, monetizing some impacts, such as the loss of personal or business information is difficult. There are several sources of cybercrime data/information available for estimating losses:

- Bureau of Justice Statistics (2008);
- PWC (2014);
- Council of Economic Advisers (2018);
- McAfee (2018) and the Center for Strategic and International Studies;
- Accenture Security (2019) and Ponemon Institute;

A number of challenges arise in regard to surveying and measuring the costs of cybercrime (Armin et al. 2015, Florencio and Herley 2016). The first is the distribution of losses, as a small number tends to account for a large proportion of losses. To illustrate this issue, consider Figure 4.1, which presents the mean for 100 trials, each with 1000 samples of a 30 000 population that has a lognormal distribution - note that no units are

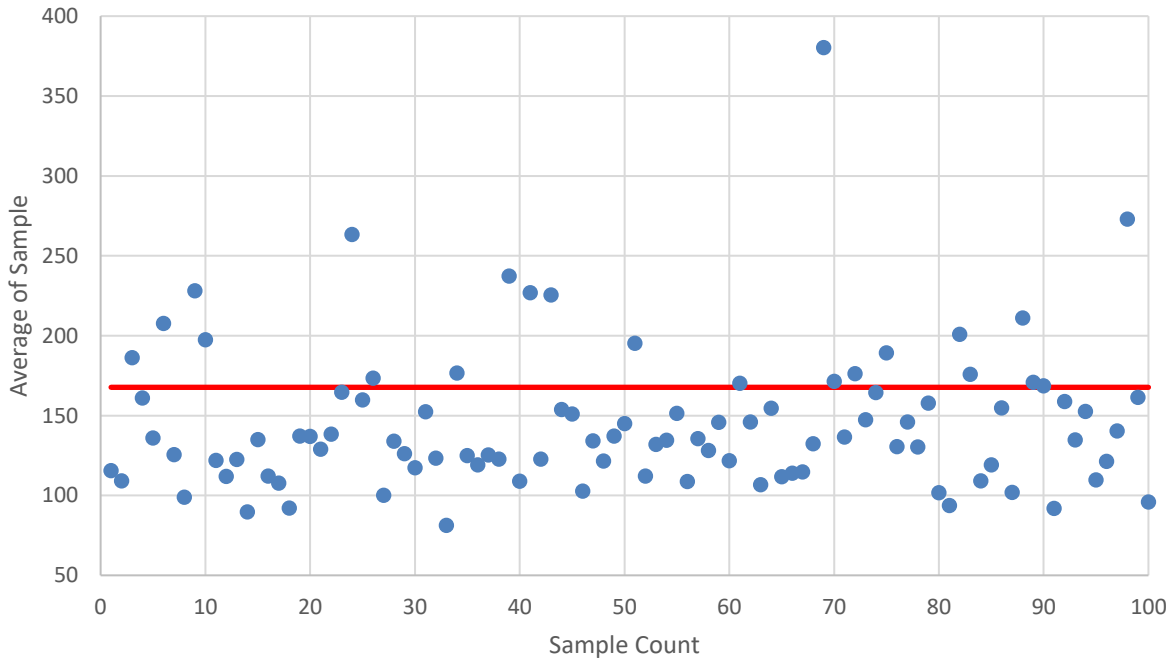

Figure 4.1: Sampling a Lognormal Distribution, Estimates of the Mean

used here, as this is an illustration of a mathematical issue. The actual mean is 167.7, as shown in the red line. The sample means vary significantly from the actual. In this example, the actual mean of the population is *higher* than the average sample means, illustrating the unreliability of the estimates. This issue is further discussed in Florencio and Herley (2016). Because of the distribution, an extremely large sample is needed to estimate the losses. A sample size of 1000 is often seen as large enough to make estimates; however, in the example above, it is not sufficient. Moreover, if an estimate of cybercrime losses relies on a small or even moderate sized sample, it will tend to underestimate the losses. Another issue that arises regarding cybercrime costs is selection bias. There is the potential for those who experience losses to be more or less likely to respond to a survey. If this issue is present, this can bias the responses. Presented below are estimates of losses due to cybercrime developed using a variety of sources and methods to address some of these challenges.

U.S. Bureau of Justice Statistics: In 2001, the U.S. Bureau of Justice Statistics piloted a survey on cybercrime, which was sent out again in 2005. The goal of this survey was to produce reliable national and industry-level estimates of computer security incidents and losses. It was cosponsored by the Bureau of Justice Statistics and the National Cyber Security Division of the U.S. Department of Homeland Security. The RAND corporation collected the data and documented this process in a report (Davis et al. 2008). Unfortunately, this program has not continued since that time. A total of 8079 businesses responded to the survey or 23 % of the 35 596 sampled out of a universe of 7.3 million total U.S. businesses. In 2005, 4500 businesses provided information on 22 million cybercrime incidents. Among the data sources on U.S. cybercrime, this likely constitutes the most reliable, as it approaches a large sample size and discloses its methods and results. Although there is a great deal of criticism for cybercrime loss estimates, few comments are directed at this dataset. Some of the other estimates for aggregated losses discussed below have smaller sample sizes or do not disclose the size, but given the source of their data (e.g., public information), it seems unlikely to be a larger sample for measuring U.S. losses. As discussed previously, a small sample is, likely, to underestimate losses.

From the survey, 3247 of the businesses incurred monetary loss totaling $867 million (Bureau of Justice Statistics 2008). The data has information on the number of respondents and the losses by 4 categories: Critical infrastructure; high risk, moderate risk, and low risk. Each of these categories contains a list of industries. Manufacturing is listed under high risk and has $118 077 of losses per respondent/business (see Table 4.1). Note that it is also listed under critical infrastructure but for this examination the high risk category will be used. These losses include those that result from any unauthorized access, intrusion, breach, compromise, or use of the company’s computer system.

Unfortunately, there is a significant difference between the average losses per respondent ($107 266) and the median losses per respondent ($6000; not shown), suggesting significant skewness in the distribution. If the losses were normally distributed, the mean and median would be closer in value. This skewness creates a challenge for estimating total losses, as sampling error and sampling bias can have significant impacts on the mean. Moreover, a large sample size is needed to estimate the losses. It is not clear if the

Table 4.1: Cybercrime Data from the Bureau of Justice Statistics

Respondents	Respondents	Sample	Losses ($Thousand)	Losses per Respondent ($)	Losses per Sample ($)
Critical Infrastructure	2719	11 694	287 600	105 774	24 594
Chemical and drug manufacturing	201	1052			
High Risk	1737	7564	205 100	118 077	27 115
Manufacturing, durable goods	503	1859			
Manufacturing, nondurable goods	327	1371			
Moderate Risk	1184	5294	76 100	64 274	14 375
Low Risk	2439	11 044	297 800	122 099	26 965
Total	8079	35 596	866 600		
Average				107 266	24 345
Median				6000	

data collected from the Bureau of Justice Statistics is large enough; however, it is among the largest data collections available on U.S. cybercrime losses. Over/under representation of high impact low frequency victims can dramatically change the estimate (Florencio and Herley 2016).

According to data from the U.S. Census Bureau, there were 249 979 manufacturing establishments in 2016 and 5.63 million for all industries (U.S. Census Bureau 2019). This is down from the estimated number of businesses presented by the 2005 Bureau of Justice Statistics survey, which estimated the total to be 7.3 million businesses. Thus, this decrease puts downward pressure on the loss estimate. To estimate losses by industry, we can match the losses per respondent (i.e., business), categorized by the four classes, to their corresponding industry. Losses can then be estimated and adjusted for inflation using the following equation:

Equation 1

$$Losses_{2016,CAT} = \frac{LOSS_{CAT}}{RESP_{CAT}} * ENT_{CAT} * \frac{CPI_{2016}}{CPI_{2005}}$$

where

$Losses_{2016}$ = The estimated losses due to cybercrime in 2016 for category CAT where CAT is either critical infrastructure, high risk, moderate risk, or low risk.

$LOSS_{CAT}$ = The total losses for category CAT reported to the U.S. Bureau of Justice Statistics in 2005 where CAT is either critical infrastructure, high risk, moderate risk, or low risk.

$RESP_{CAT}$ = The total number of respondents for category CAT reported to the U.S. Bureau of Justice Statistics in 2005 where CAT is either critical infrastructure, high risk, moderate risk, or low risk.

ENT_{CAT} = The total number of enterprises within category CAT in 2016 reported in the U.S. Census Bureau's Annual Survey of Entrepreneurs (U.S. Census 2019a).

CPI_{2016} = The consumer price index for all consumers from the Bureau of Labor Statistics

This approach aids in addressing any industry specific impacts that might be present, as the CAT categories are groupings of industries listed in the Bureau of Justice Statistics report (2008). After adjusting for inflation, an estimate of $36.3 billion in annual losses, or 1.5% of value added, is estimated for manufacturing and $746.2 billion for the U.S. economy, as seen in Table 4.2. Four additional estimates are provided in this table. The first uses the lowest value for losses per respondent as calculated using the categories (i.e., CAT). The lowest value is $64 274 for all industries, which is the "moderate risk" category. This value replaces $\frac{LOSS_{CAT}}{RESP_{CAT}}$ in Equation 1. The second uses an average for all respondents, $107 266, which is shown in Table 4.1. This value is also used in place of $\frac{LOSS_{CAT}}{RESP_{CAT}}$. The Bureau of Justice Statistics' risk levels were based on risk of incidents, loss, and downtime. Loss per business does not consider downtime; therefore, the lowest value may not coincide with the lowest risk category.

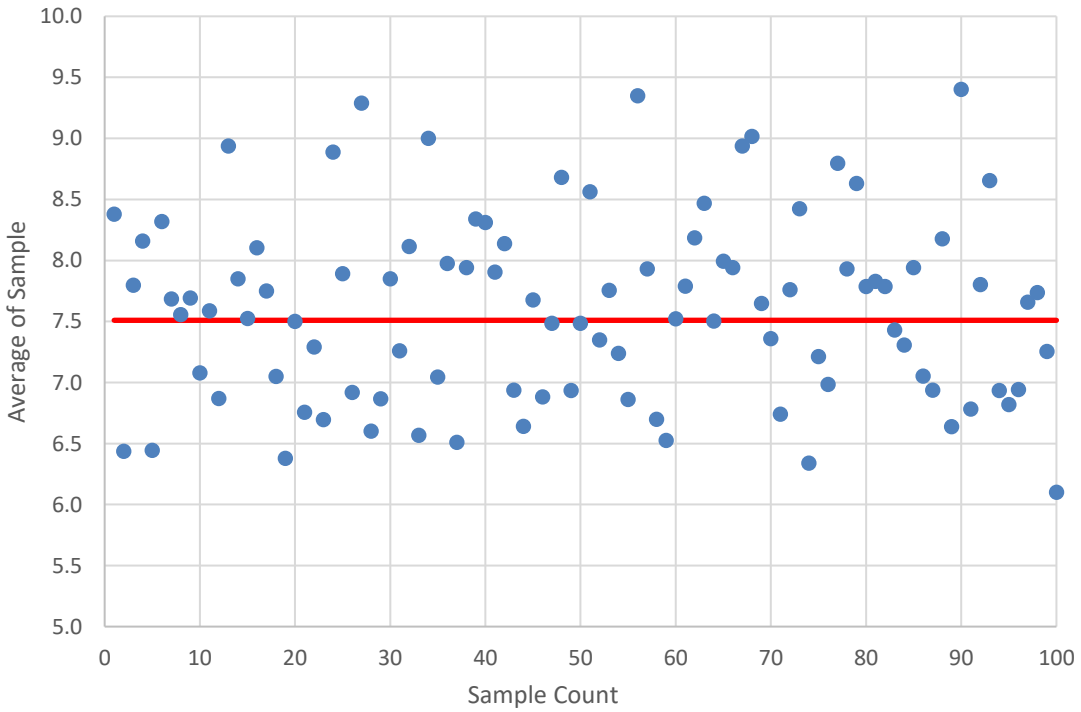

Figure 4.2: Sampling a Lognormal Distribution, Estimates of the Median

Table 4.2: Estimated Losses Using U.S. Bureau of Justice Statistics Data, 2016

Industry	Firms#	Respondent Category	2005 Losses per Respondent ($000's)	Losses ($Billions)*	Losses - Using Low ($Billions)*	Losses - Using Avg ($Billions)*	Losses - Using Median ($Billions)*	Losses - Using Sample ($Billions)*
Agriculture, forestry, fishing and hunting	27 210	Critical Infrastructure	105.8	3.5	2.1	3.6	0.2	0.8
Mining, quarrying, and oil and gas extraction	22 405	Low Risk	122.1	3.4	1.8	3.0	0.2	0.7
Utilities	6 080	Critical Infrastructure	105.8	0.8	0.5	0.8	0.0	0.2
Construction	665 397	Low Risk	122.1	99.8	52.6	87.7	4.9	22.0
Manufacturing	249 979	High Risk	118.1	36.3	19.7	33.0	1.8	8.3
Wholesale trade	306 088	High Risk	118.1	44.4	24.2	40.3	2.3	10.2
Retail trade	650 266	High Risk	118.1	94.4	51.4	85.7	4.8	21.7
Transportation and warehousing	182 236	Critical Infrastructure	105.8	23.7	14.4	24.0	1.3	5.5
Information	73 722	Critical Infrastructure	105.8	9.6	5.8	9.7	0.5	2.2
Finance and insurance	235 362	Critical Infrastructure	105.8	30.6	18.6	31.0	1.7	7.1
Real estate and rental and leasing	290 157	Critical Infrastructure	105.8	37.7	22.9	38.2	2.1	8.8
Professional, scientific, and technical services	800 201	Moderate Risk	64.3	63.2	63.2	105.5	5.9	14.1
Management of companies and enterprises	25 848	Low Risk	122.1	3.9	2.0	3.4	0.2	0.9
Administrative and support and waste management and remediation services	334 255	Low Risk	122.1	50.2	26.4	44.1	2.5	11.1
Educational services	90 789	Moderate Risk	64.3	7.2	7.2	12.0	0.7	1.6
Health care and social assistance	646 042	Critical Infrastructure	105.8	84.0	51.0	85.2	4.8	19.5
Arts, entertainment, and recreation	121 254	Low Risk	122.1	18.2	9.6	16.0	0.9	4.0
Accommodation and food services	517 676	Low Risk	122.1	77.7	40.9	68.2	3.8	17.2
Other services (except public administration)	385 357	Low Risk	122.1	57.8	30.4	50.8	2.8	12.8
TOTAL	5 630 324			746.2	444.7	742.2	41.5	168.8

Firm is synonymous with company (U.S. Census 2019b)

* Adjusted to 2016 using the Consumer Price Index

The last two estimates were developed to establish a lower bound estimate for cybercrime losses. Both estimates would be expected to be lower than the true impact of cybercrime; so, the higher of the two can be used as a lower bound. The first uses the median, as the losses per respondent. In a distribution with a long right tail, the median tends to be less than the mean; thus, the median would tend to be a lower bound estimate. Also, the median would tend to be represented more accurately in the sample of a lognormal distribution because the median is not as sensitive to extreme values (Hozo et al. 2005). For instance, using the same data from Figure 4.1, we can develop 100 samplings to estimate the median of our population of 30 000. As illustrated in Figure 4.2, the median is more accurately represented. The true median, shown in red is 7.5 while the average of the medians of the samples is 7.6, a difference of 1.3 %.

The last estimate assumes that all those in the sample that did not respond to the survey, experienced no cybercrimes and had zero losses. This increases $RESP_{CAT}$ to 11 694 respondents for critical infrastructure, 7564 for high risk, 5294 for moderate risk, and 11 044 for low risk for a total of 35 596 respondents. Because we assume that all those in the sample responded, the effect of oversampling of those who experienced cybercrime losses is eliminated. Since we assume that the additional respondents had zero losses, we reduce/eliminate the effect of any over estimation of losses that respondents might have had. The per business losses amount to $25 594 for critical infrastructure, $27 115 for high risk, $14 375 for moderate risk, and $26 965 for low risk. The losses that businesses believe they lost due to cybercrime for the 35 596 businesses sampled should not be less than these values, as the non-respondents are assumed to have zero losses and, presumably, losses cannot be negative (i.e., by definition, losses should not be gains). This estimate sets the floor at $168.8 billion in losses.

Given the wide ranges of the data from the U.S. Bureau of Justice Statistics, a probabilistic sensitivity analysis using Monte Carlo analysis was conducted to examine the impact of fluctuating different variables. This technique is based on works by McKay, Conover, and Beckman (1979) and by Harris (1984) that involves a method of model sampling. Specification involves defining which variables are to be simulated, the distribution of each of these variables, and the number of iterations performed. The software then randomly samples from the probabilities for each input variable of interest. This analysis utilized NIST's Monte Carlo Tool to conduct the simulation (NIST 2019).

A number of variables were included in the simulation. Some industries matched more than one category (CAT). For instance, *finance and insurance* could fit in *critical infrastructure* or *moderate*, as finance is in one while insurance is in the other. Recall that the categories are groupings of industries, specified in the Bureau of Justice Statistics report (2008). In instances where an industry fit into two categories, a discrete uniform distribution was used where each of the possible categories had an equal probability. Matchings are shown in Table 4.3. The adjustment for inflation $\frac{CPI_{2016}}{CPI_{2005}}$ was varied using a triangular distribution where the low was 10 % lower than the measured value and the high was 10 % higher. The mode was the original value. Inflation was included in the Monte Carlo analysis because the basket of goods used in the Consumer Price Index does

Table 4.3: Industries and Corresponding Categories for Monte Carlo Analysis

Industry	Category 1	Category 2
Agriculture, forestry, fishing and hunting	Critical Infrastructure	
Mining, quarrying, and oil and gas extraction	Low Risk	Critical Infrastructure
Utilities	Critical Infrastructure	
Construction	Low Risk	
Manufacturing	High Risk	Critical Infrastructure
Wholesale trade	High Risk	
Retail trade	High Risk	
Transportation and warehousing	Low Risk	Critical Infrastructure
Information	High Risk	Critical Infrastructure
Finance and insurance	Moderate Risk	Critical Infrastructure
Real estate and rental and leasing	Low Risk	Critical Infrastructure
Professional, scientific, and technical services	Moderate Risk	High Risk
Management of companies and enterprises	Low Risk	
Administrative and support and waste management and remediation services	Low Risk	
Educational services	Low Risk	Moderate Risk
Health care and social assistance	Low Risk	Critical Infrastructure
Arts, entertainment, and recreation	Low Risk	
Accommodation and food services	Low Risk	
Other services (except public administration)	Low Risk	

not match those represented by cybercrime losses. Also included in the analysis is the number of firms in each industry, which is varied by plus/minus 10 % using a triangular distribution. Finally, the number of respondents, $RESP_{CAT}$, included in the estimate of losses per firm was varied between the actual number of respondents to the Bureau of Justice Statistics survey and the total number sampled using a uniform distribution. The variables included are summarized in Table 4.4.

The results of the Monte Carlo analysis are presented in Figure 4.3. The lowest value in the simulation was $167.9 billion in losses. As will be seen later, even this low estimate exceeds most other estimates such as that made by the Council of Economic Advisers

Table 4.4: Variables included in Monte Carlo Analysis

Variable	Distribution	Low	Mode	High
Category Inclusion	Uniform	n/a	n/a	n/a
CPI	Triangular	10 % lower	Estimate	10 % higher
Number of Firms	Triangular	10 % lower	Estimate	10 % higher
Survey Respondents	Uniform	Actual Value	n/a	Total Sampled

(2018) and McAfee (2018), which have high levels of uncertainty, as acknowledged in their reports. One issue that has been raised as a source of differences in loss estimates is the definitions used. McAfee and the Bureau of Justice Statistics each have their own definitions (see Appendix A); however, these definitions have significant similarities.

Approximately 90 % of the values in the Monte Carlo simulation are below $473 billion. The median is $318.1 billion, which means that 50 % of the simulations were below this value. The high was $770.0 billion. The simulation tends to favor lower values over higher values. For instance, 27.3 % of the simulations fall into the first $100 billion that range from the lowest value of $167.9 billion to $267.9 billion. Meanwhile, only 0.2 % of the simulations fall into the last $100 billion from $670.0 billion to $770.0 billion. Since the data from the Bureau of Justice Statistics is from 2005, these estimates are likely low, as the digital economy grew 129 % between 2005 and 2016 (Bureau of Economic Analysis 2020).

One concern that has been raised is that estimates of losses from cybercrime are inflated due to monetizing intellectual property theft, where criminals do not always gain the full value of stolen property (McAfee 2018). The Bureau of Justice Statistics data estimates theft of intellectual property as being 18.4 % of losses and is not the largest source of loss. If we take the low estimate from the Monte Carlo analysis and subtract off 18.4 %

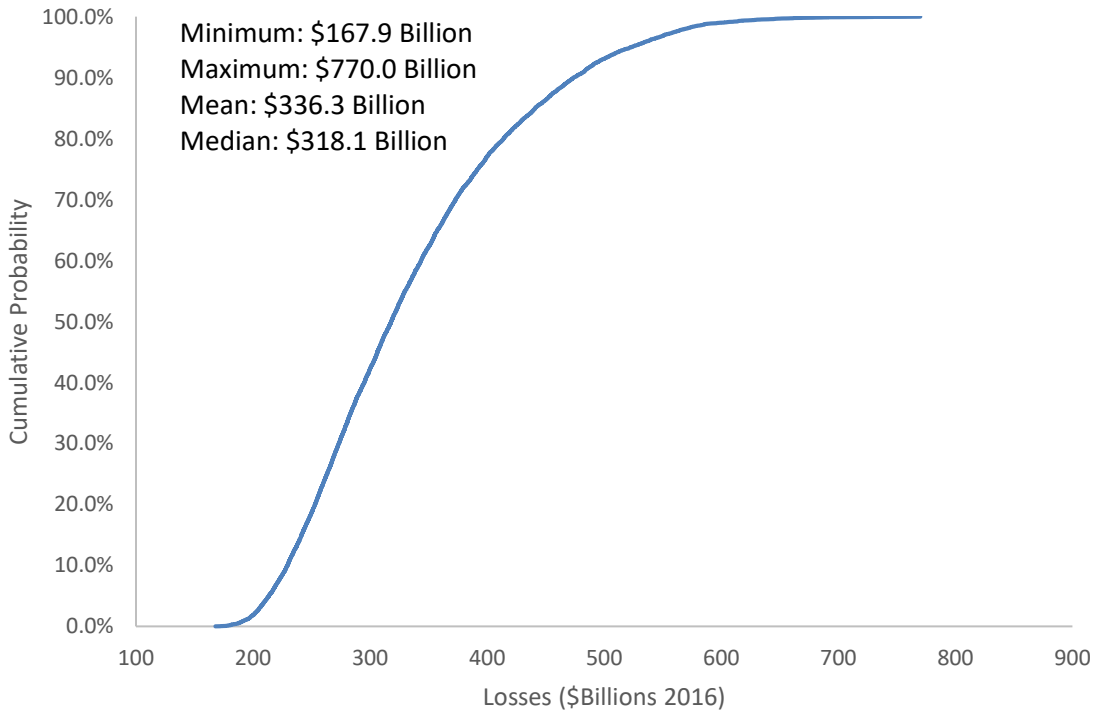

Figure 4.3: Cumulative Probability Graph of Losses, Monte Carlo Results

(i.e., all losses due to intellectual property theft), the total is $137.0 billion, which still exceeds the McAfee estimate of 0.64 % of GDP (i.e., $119.8 billion in 2016).

PWC: PWC estimated that the average financial loss attributed to cybersecurity incidents was $2.7 million in 2014 (PWC 2014). For small, medium, and large organizations (not defined), losses were around $0.41 million, $1.3 million, and $5.9 million, respectively. The methodology used by PWC was only discussed briefly and it was not clear whether efforts were made to reduce the effect of self-selection or other survey data challenges. Their estimates were based on over 9700 respondents to a survey, which suggests that it might have a sample size large enough to avoid some of the previously mentioned data issues; however, it is not clear how many businesses this represented. Also, the data/results presented do not lend themselves to making national aggregated estimates. A lower bound estimate of total losses might be made by taking the small organization losses (i.e., $0.41 million) and multiplying it by the number of enterprises that had monetary losses:

Equation 2

$$Losses_{2016} = PROP_{2005} ENT_{TOT} * 0.41 * \frac{CPI_{2016}}{CPI_{2014}}$$

where

$PROP_{2005}$ = The proportion (79 %) of businesses that reported having monetary loss in the Bureau of Justice Statistics data discussed above

ENT_{TOT} = Total number of enterprises in 2016 from U.S. Census Bureau's Annual Survey of Entrepreneurs

One could make the assumption discussed previously that all non-respondents in the Bureau of Justice Statistics data experienced zero losses due to cybercrime. However, this would only partially address the potential effect of self-selection and would not address the impact of any over estimates made by respondents. Moreover, due to the self-selection bias and potential for over estimation by respondents, a true lower bound estimate could not be made using the PWC data. Another issue with this method is that the per organization damage estimate is a global estimate and this report is aimed at measuring U.S. cybercrime losses.

Council of Economic Advisers: According to the Council of Economic Advisers to the president, malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016 (Council of Economic Advisors 2018); however, the method for estimating this value was not readily discussed. Using news reports on cyberattacks and data breaches, they also estimated that an adverse cyber event resulted in an approximate 0.8 % decline in their market value in the seven days that followed the event with the average loss being $498 million. These results, however, are likely to be heavily skewed towards large firms and events of large cost magnitude since they depend on news reports. The Council of Economic Advisers also concluded that cyber security is "plagued by insufficient data."

McAfee and the Center for Strategic and International Studies: According to this report from the Center for Strategic and International Studies estimates that cybercrime was 0.64 % of U.S. GDP in 2013 (Center for Strategic and International Studies 2014). In 2016, 0.64 % of GDP amounted to $119.8 billion. Unfortunately, the method or source for determining this estimate was only generally discussed. A second report released from the same organization in 2018 estimated that there were between $140 billion and $175 billion or between 0.69 % and 0.87 % of GDP lost to cybercrime in North America (McAfee 2018). These reports used "publicly available information on national losses, finding data on roughly 50 countries" (McAfee 2018 p. 3). Beyond this statement, only limited information on methods/data for estimating losses were disclosed. Given the absence of data on cybercrime, as acknowledged by those who research this issue, including McAfee, it is unlikely that these estimates are based on a large sample size; thus, it is likely that this estimate underestimates cybercrime losses.

In their 2013 report, they indicated that they, "use several analogies where costs have already been quantified to provide an idea of the scope of the problem, allowing us to set rough bounds—a ceiling and a floor—for the cost of malicious cyber activity, by comparing it to other kinds of crime and loss" (Center for Strategic and International Studies 2013). Further, they assume that cybercrime, "falls into the same range as car crashes, pilferage, and drugs, [AND] this is a "ceiling" for an estimate of loss" (Center for Strategic and International Studies 2013). A similar assumption is stated in the 2018 report in that their, "assumption is that cybercrime mirrors other criminal activities." (Center for Strategic and International Studies 2018). Stated another way, there is an assumption that the losses cannot exceed other losses experienced in society. This may or may not actually be the case.

These reports are among the more cited estimates. For instance, as of January 14, 2020, when searching Google for "economic impact of cybercrime," the 2018 report accounts for the first 10 items, accounting for the first full page of results. In reviewing relevant literature, they were commonly cited.

Accenture Security and Ponemon: For firms with 5000 or more employees (referred to as seats) or more, an individual company/organization experienced, on average, 145 security breaches in 2018, up 11 % from 2017 (Accenture Security 2019). These breaches cost the company/organization an average of $13.0 million in 2018, which is 12 % higher than in 2017 and 72 % higher over the last five years. This excludes attacks that were stopped by a company's firewall or other means. In 2018, the automotive and high-tech industries experienced slightly higher impacts, as seen in Table 4.5. The estimated total value at risk (cumulative from 2019 to 2023) is $5.2 trillion with high tech at $753 billion and automotive at $505 billion (Accenture Security 2019). The value at risk equates to 2.8 % of revenue. There is only limited discussion on addressing oversampling or other data challenges; therefore, it is not clear to the extent that this is an issue in this data. The report does indicate that senior leaders from 355 companies were interviewed, making this a small sample size.

Table 4.5: Average Total Cost of Breaches (per company/organization) $million

	2017	2018	Percent Change
Total	11.7	13.0	11.1%
Automotive	10.7	15.8	47.5%
High Tech	12.9	14.7	13.9%
Consumer Goods	8.1	11.9	47.2%

Source: Accenture Security (2019) The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study. https://www.accenture.com/us-en/insights/security/cost-cybercrime-study
Note: Pertains to companies/organizations with 5000 or more seats

Combining the estimates from Accenture Security with the total number of firms with 5000 or more employees can provide some insight into the total impact of cybercrime. Unfortunately, the data from the U.S. Census Bureau (2019) does not separate information on firms with 5000 or more employees; however, this information might be forecasted. One can use the breakout of other firm sizes to predict this value by graphing and modeling the number of firms by the minimum number of employees in the group. The structural equation would be the following:
Equation 3

$$MNE = \beta_1 F^x + \beta_2 + \mathcal{E}$$

where
MNE = Minimum number of employees from the ranges set by the U.S. Census Bureau (see Table 4.6)
F = Number of firms above the minimum number of employees (see Table 4.6)
β = Parameters to be estimated
x = Parameter to be estimated
$\mathcal{E}$ = Error term

Table 4.6: Data for Model of Establishments by Size

U.S. Census Bureau Data		Altered Data	
U.S. Census Bureau Range	Number of Firms	Firms with more than (MNE)	Number of Firms (F)
Firms with 1 to 4 employees	2 736 389	-	-
Firms with 5 to 9 employees	927 950	4	2 078 972
Firms with 10 to 19 employees	567 334	9	1 151 022
Firms with 20 to 49 employees	366 663	19	583 688
Firms with 50 to 99 employees	116 988	49	217 025
Firms with 100 to 499 employees	82 313	99	100 037
Firms with 500 employees or more	17 724	499	17 724

Figure 4.4 presents the number of firms by minimum number of employees. Using a basic Excel power trend line, an equation can be used to predict the number of firms with 5000 or more employees (see the equation in Figure 4.4). The value for F can be replaced with 4999 to calculate the number of firms with 5000 or more employees. The result is an estimated 1967 establishments.

Using Accenture Security's estimate of $13 million in cybersecurity damages per firm, an estimate of $25.6 billion in total damages is estimated for firms with 5000 or more employees in the U.S. This damage estimate is only for a fraction of the economy, as firms with over 5000 employees represents only 0.04 % of all firms. This is likely an overestimate, as Accenture Security uses the term "seats" rather than employees, suggesting that these might be computer seats. Thus, it might actually only apply to companies with even more than 5000 employees.

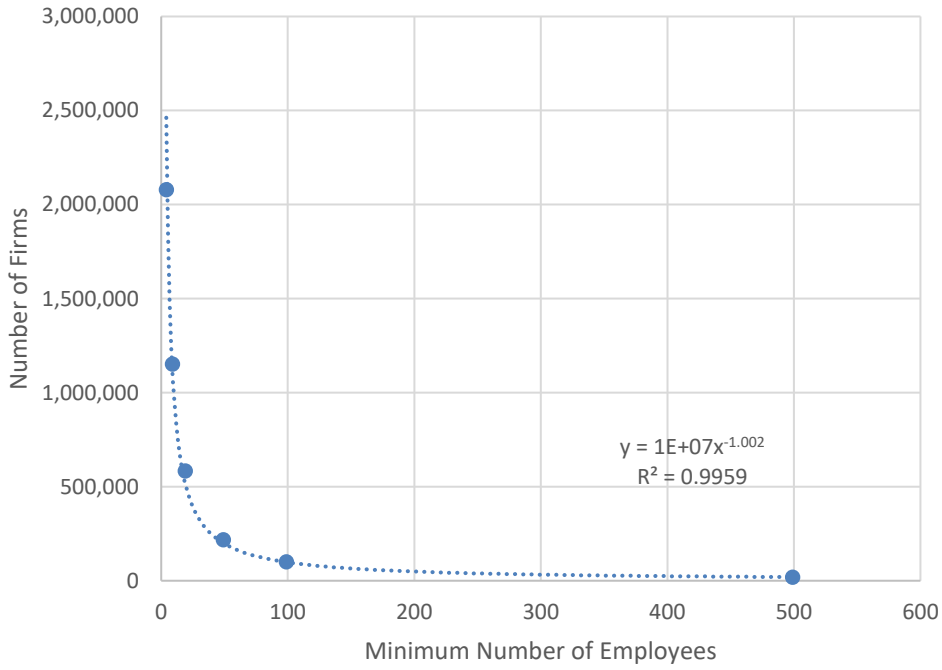

Figure 4.4: Number of Firms by Minimum Number of Employees

5. Summary

Estimations made in this report, which documents both the methods and data used, suggest an economic impact from cybercrimes in the U.S. of between 0.9 % and 4.1 % of GDP, a substantial loss. For manufacturing, the loss is between $8.3 billion and $36.3 billion (i.e., 0.4 % and 1.7 % of value added). These estimates were developed using public data from the Bureau of Justice Statistics and employ uncertainty analysis methods. These estimates exceed those of many others (see Table 5.1), which tend to have limited disclosure of methods/data and tend not to examine uncertainty, at least publicly. Additionally, other estimates may rely on small sample sizes, which is problematic for examining losses due to criminal activity or do not lend themselves to estimating aggregated national losses. The more widely cited estimate, which is from McAfee (2014), is that cybercrime amounts to 0.64 % of U.S. GDP or $119.8 billion in 2016 .

The low estimate of $167.9 billion (i.e., 0.9 % of GDP) is based on unrealistic assumptions, which create a lower boundary that has downward bias, as we assumed that of the 36 000 businesses surveyed by the Bureau of Justice Statistics, those who did not respond, experienced no losses. Still, the low is 40 % higher than the McAfee estimate. The assumption amounted to 77 % of the sample being presumed as having no loss; thus, the true loss is almost certainly higher than the low estimate. The high estimate of $770.0 billion, likely, suffers from selection bias and other issues, making it an upper bound estimate. Although it is possible that the true loss approaches this level, the results from a Monte Carlo simulation put 90 % of the values below $473 billion or 2.5 % of GDP, based on the methods used here. If the Bureau of Justice Statistics data is representative, then the losses amount to $770 billion.

Future research can focus on more rigorous data collection and analysis. The Bureau of Justice Statistics' National Computer Security Survey provides a great source of data; however, this collection has not continued since 2005. Publications on cybercrime have a tendency to be summary reports; however, given the current state of knowledge, more rigorous disclosure of methods and analysis are needed. Without an understanding of the losses that result from cybercrime, it is unclear what level of resources public and private entities should allocate toward mitigation and prevention. There is a great deal at risk, including trillions of dollars in assets and economic activity, not to mention the implications for national security, which was not discussed in this report.

Table 5.1: Estimates of Losses Due to Cybercrime

Description	Losses	% of Value Added	Sources	Disclosed Technical Details of Method and Data	Sample Size
2016 Cybercrime losses (manufacturing)	$8.3 Billion - $36.3 Billion	0.4% - 1.7%	Data: Bureau of Justice Statistics 2005	Yes	4500
2016 Cybercrime losses	$167.9 Billion - $770.0 Billion	0.9% - 4.1%	Data: Bureau of Justice Statistics 2005	Yes	4500
2013 Cybercrime losses	$107.4 Billion	0.64%	Center for Strategic and International Studies 2014	Limited	Unknown - Aggregated Public Data
2016 Cybercrime losses	$57 Billion - $109 Billion	0.31% - 0.58%	Council of Economic Advisors 2018	Limited	Unknown
2017 Cybercrime losses (North America)	$140 Billion - $175 Billion	0.69% - 0.87%	McAfee 2018	Limited	Unknown - Aggregated Public Data
2018 Cybercrime losses (Firms with 5000 or more employees = 0.04 % of all firms)	$25.6 Billion	-	Data: Accenture Security 2019	Limited	355 Companies
2018 per company losses	Total: $13.0 Million Auto: $15.8 Million High Tech: $14.7 Million Consumer Goods: $11.9 Million	-	Data: Accenture Security 2019	Limited	355 Companies
2014 Per incident loss	Small Firm: $0.41 Million Medium Firm: $1.3 Million Large Firm: $5.9 Million	-	PWC 2014	Limited	9700 Respondents
2016 Per Incident loss (skewed toward large firms and noteworthy incidents)	$498 Million (0.8% of market value)	-	Council of Economic Advisors 2018	Yes	186 Firms

Acknowledgments

The author wishes to thank all those who contributed so many excellent ideas and suggestions for this report. Special appreciation is extended to Keith Stouffer of the Engineering Laboratory's Intelligent Systems Division for his technical guidance and suggestions. Special appreciation is also extended to Dr. David Butry and Dr. Jennifer Helgeson of the Engineering Laboratory's Applied Economics Office for their thorough reviews and many insights. The author also wishes to thank Dr. Nicos Martys, Materials and Structural Systems Division, for his review.

References

Accenture Security (2019) The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study. https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

Allianz. (2020) Allianz Risk Barometer: Identifying the Major Business Risks for 2020. https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html

Anderson, Ross, Chris Barton, Rainer Bohme, Richard Clayton, Miche J.G. van Eeten, Michael Levi, Tyler Moore, and Stefan Savage. Measuring the Cost of Cybercrime. https://www.econinfosec.org/archive/weis2012/papers/Anderson_WEIS2012.pdf

Armin, Jart, Bryn Thompson, David Ariu, Giorgio Giacinto, Fabio Roli, Piotr, Kijewski. 2020 Cybercrime Economic Costs: No Measure No Solution. 2015. 10th International Conference on Availability, Reliability, and Security. https://ieeexplore.ieee.org/document/7299982

Bureau of Economic Analysis (2019). Fixed Assets. https://apps.bea.gov/iTable/index_FA.cfm

Bureau of Economic Analysis (2020). Digital Economy. https://www.bea.gov/data/special-topics/digital-economy

Bureau of Justice Statistics (2008). Cybercrime against Businesses, 2005. https://www.bjs.gov/content/pub/pdf/cb05.pdf

Center for Strategic and International Studies (2013). The Economic Impact of Cybercrime and Cyber Espionage. McAfee. https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf

Center for Strategic and International Studies (2014). Net Losses: Estimating the Global Cost of Cybercrime – Economic Impact of Cybercrime II. https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf

Council of Economic Advisors (2018) The Cost of Malicious Cyber Activity to the U.S. Economy. White House. https://www.whitehouse.gov/articles/cea-report-cost-malicious-cyber-activity-u-s-economy/

Davis, Lois M., Daniela Golinelli, Robin Beckman, Sarah K. Cotton, Robert H. Anderson, Anil Bamezai, Christopher R. Corey, Megan Zander-Cotugno, John L. Adams, Roald Euller, and Paul Steinberg (2008). The National Computer Security Survey (NCSS). RAND. https://www.rand.org/content/dam/rand/pubs/technical_reports/2008/RAND_TR544.pdf

Eling, Martin and Werner Schnell (2016). What do we Know about Cyber Risk and Cyber Risk Insurance? Journal of Risk Finance. 17(5).

https://www.emerald.com/insight/content/doi/10.1108/JRF-09-2016-0122/full/html?fullSc=1

Florencio, Diei and Cormac Herley. Sex, Lies and Cyber-Crime Surveys. (2016). Microsoft Research. https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/SexLiesandCybercrimeSurveys.pdf

Forbes (2014). Fallout: The Reputational Impact of IT Risk. https://images.forbes.com/forbesinsights/StudyPDFs/IBM_Reputational_IT_Risk_REPORT.pdf

Frontier Economics Ltd. (2011) Estimating the Global Economic and Social Impacts of Counterfeiting and Piracy: A Report Commissioned by Business Action to Stop Counterfeiting and Piracy. https://cdn.iccwbo.org/content/uploads/sites/3/2016/11/ICC-BASCAP-Global-Impacts-Full-Report-2011.pdf

Harris, C. M. Issues in Sensitivity and Statistical Analysis of Large-Scale, Computer-Based Models, NBS GCR 84-466, Gaithersburg, MD: National Bureau of Standards, 1984.

Hozo, Stela Pudar, Benjamin Djulbegovic, and Iztok Hozo. “Estimating the Mean and Variance from the Median, Range, and the Size of a Sample.” BMC Medical Research Methodology. 5(13). https://doi.org/10.1186/1471-2288-5-13

Hyman, Paul. Cybercrime: It’s Serious, But Exactly How Serious? Communications of the ACM. 56(3). https://dl.acm.org/doi/pdf/10.1145/2428556.2428563

Intel Security (2014) Net Losses: Estimating the Global Cost of Cybercrime: Economic Impact of Cybercrime II. https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf

Jardine, Eric (2015). Global Cyberspace is Safer than You Think: Real Trends in Cybercrime. https://www.cigionline.org/sites/default/files/no16_web_0.pdf

MAKE UK (2018). Cyber Security for Manufacturing. https://www.makeuk.org/insights/reports/2019/02/11/cyber-security-for-manufacturing

McAfee (2018). Economic Impact of Cybercrime – No Slowing Down. https://www.csis.org/analysis/economic-impact-cybercrime

McKay, M. C., Conover, W. H., and Beckman, R.J. “A Comparison of Three Methods for Selecting Values of Input Variables in the Analysis of Output from a Computer Code,” Technometrics 21 (1979): 239-245.

NIST (2019). Monte Carlo Tool. https://www.nist.gov/services-resources/software/monte-carlo-tool

PWC (2014) Managing Cyber Risks in an Interconnected World. https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf

PWC (2020) Navigating the Rising Tide of Uncertainty. 23rd Annual Global CEO Survey. https://www.pwc.com/gx/en/ceo-agenda/ceosurvey/2020.html and www.ceosurvey.pwc

U.S. Census Bureau (2019a). Annual Survey of Entrepreneurs. https://www.census.gov/programs-surveys/ase.html

U.S. Census Bureau (2019b). Annual Survey of Entrepreneurs: Methodology. https://www.census.gov/programs-surveys/ase/technical-documentation/methodology.html

Verizon (2019) 2019 Data Breach Investigations Report. https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

Appendix A: Definitions

General Category	McAfee	Bureau of Justice Statistics
Means of cybercrime	Criminals gaining illicit access to a victim's computer.	Security incidents in which a computer was used as the means of committing a crime against the company.
Fraud and Financial	Online fraud and financial crimes, often the result of stolen personally identifiable information (PII)	Fraud—the intentional misrepresentation of information or identity to deceive others, the unlawful use of a credit or debit card or ATM, or the use of electronic means to transmit deceptive information, in order to obtain money or other things of value. Fraud may be committed by someone inside or outside the business. Includes instances in which a computer was used to defraud the business of money, property, financial documents, insurance policies, deeds, use of rental cars, or various services by forgery, misrepresented identity, credit card or wire fraud. Excludes incidents of embezzlement. Theft of intellectual property—the illegal obtaining of copyrighted or patented material, trade secrets, or trademarks (including designs, plans, blueprints, codes, computer programs, software, formulas, recipes, graphics) usually by electronic copying. Excludes theft of personal or financial data such as credit card or social security numbers, names and dates of birth, financial account information, or any other type of information.
	Financial manipulation, using stolen sensitive business information on potential mergers or advance knowledge of performance reports for publicly traded companies	Embezzlement—the unlawful misappropriation of money or other things of value, by the person to whom the property was entrusted (typically an employee), for his or her own purpose. Includes instances in which a computer was used to wrongfully transfer, counterfeit, forge or gain access to money, property, financial documents, insurance policies, deeds, use of rental cars, or various services by the person to whom they were entrusted.
		Theft of personal or financial data—the illegal obtaining of information that potentially allows someone to use or create accounts under another name (individual, business, or some other entity). Personal information includes names, dates of birth, social security numbers, or other personal information. Financial information includes credit, debit, or ATM card account or PIN numbers. Excludes theft of intellectual property such as copyrights, patents, trade secrets, and trademarks. Excludes theft of any other type of information. Other computer security incidents—Incidents that do not fit within the definitions of the specific types of cyber-attacks and cyber theft. Encompasses spyware, adware, hacking, phishing, spoofing, pinging, port scanning, sniffing, and theft of other information, regardless of whether damage or losses were sustained as a result.
Business Interruption and Recovery	Opportunity costs, including disruption in production or services, and reduced trust for online activities. This includes the effect of ransomware, which involves both payments to redeem encrypted data, and, more importantly, serious disruptions to services and output.	Computer virus—a hidden fragment of computer code which propagates by inserting itself into or modifying other programs. Includes viruses, worms, and Trojan horses. Excludes spyware, adware, and other malware.

	The cost of securing networks, buying cyber insurance, and paying for recovery from cyberattacks	Denial of service—the disruption, degradation, or exhaustion of an Internet connection or e-mail service that results in an interruption of the normal flow of information. Denial of service is usually caused by ping attacks, port scanning probes, or excessive amounts of incoming data. Electronic vandalism or sabotage—the deliberate or malicious damage, defacement, destruction or other alteration of electronic files, data, web pages, or programs.
Other	Reputational damage and liability risk for the hacked company and its brand, including temporary damage to stock value	

Appendix B: 2005 National Computer Security Survey

FORM **NCSS-1**
(4/24/06)

OMB No. 1121-0301: Approval Expires 08/31/2008

2005 NATIONAL COMPUTER SECURITY SURVEY

RETURN COMPLETED FORM TO:
RAND Corporation
Survey Research Group
1776 Main Street
P.O. Box 2138
Santa Monica, CA 90407-2138

OR
FAX TO:
1-877-814-6673

For assistance
Phone: 1-800-734-5399
Monday through Friday
8:00 a.m. to 5:00 p.m. Pacific Time
OR
E-mail: ncss@rand.org

NOTICE OF CONFIDENTIALITY—Your report is confidential by law (P.L. 107-347, Title V and 44 U.S.C. § 3501 note). It may be seen only by persons certified to uphold the confidentiality of information and used only for statistical purposes from which no firm may be identified. The law also prohibits the sharing of your data with other agencies, exempts the information you provide from requests made under the Freedom of Information Act, and ensures that your responses are immune from legal process.

U.S. DEPARTMENT OF JUSTICE
BUREAU OF JUSTICE STATISTICS

In partnership with the

U.S. DEPARTMENT OF HOMELAND SECURITY
NATIONAL CYBER SECURITY DIVISION

SURVEY SCOPE
This voluntary survey collects data on the type and frequency of computer security incidents in which a computer was used as the means of committing a crime against the company.

REPORTING ENTITY
Report consolidated figures for DOMESTIC OPERATIONS of this company, including all DIVISIONS and LOCATIONS, and **excluding** SUBSIDIARIES. *Use figures that include subsidiaries only if figures excluding subsidiaries are not available.* For this survey, subsidiary means a company in which this company has more than 50% ownership, or in which this company has the power to direct or cause the direction of management and policies.

REPORTING PERIOD
The reporting period for this survey is CALENDAR YEAR 2005. If 2005 calendar year figures are not available, please use fiscal year 2005 data.

ESTIMATES
If exact figures are not available, estimates are acceptable.

Use a dark colored pen to fill out the survey. Completely fill in the squares ■ or circles ● to indicate your responses. To indicate an answer selected in error, draw a heavy "X" over the square or circle. When reporting a number, avoid writing on the edge of the response box. Please refer to the instructions on page 14 before completing the survey.

I. COMPUTER SECURITY CONCERNS

1a. What are the top three computer security concerns for this company? *Mark ■ up to three.*

- ☐ Computer virus, worm, or Trojan horse
- ☐ Denial of service
- ☐ Electronic vandalism or sabotage
- ☐ Embezzlement
- ☐ Fraud
- ☐ Theft of intellectual property (copyrights, patents, trade secrets, trademarks)
- ☐ Unlicensed use or copying (piracy) of digital products—software, music, motion pictures, etc.—developed for resale
- ☐ Theft of personal or financial information such as names and dates of birth; social security numbers; credit/debit/ATM card, account, or PIN numbers; etc.
- ☐ Other computer security incidents such as hacking, spoofing, phishing, sniffing, pinging, scanning, spyware, adware, other malware, etc.
- ☐ Misuse of computers by employees (Internet, e-mail, etc.)
- ☐ Breaches resulting from information obtained from stolen laptops
- ☐ Other → Specify: _____

b. What three potential sources of computer security threat are of greatest concern to this company? *Mark ■ up to three.*

- ☐ Current employee
- ☐ Current contractor, vendor, temporary worker, etc.
- ☐ Former employee, contractor, vendor, temporary worker, etc.
- ☐ Domestic competitor
- ☐ Foreign competitor
- ☐ Domestic hacker
- ☐ Foreign hacker
- ☐ Other → Specify: _____

II. COMPUTER INFRASTRUCTURE & SECURITY

2a. In 2005, what types of computer networks (including Internet) or equipment did this company use?
For this survey, "company" means DOMESTIC OPERATIONS, including all DIVISIONS and LOCATIONS. *Mark ■ all that apply.*

- ☐ Local area network (LAN)
- ☐ Wide area network (WAN)
- ☐ Process control network (PCN)
- ☐ Virtual private network (VPN)
- ☐ Wireless network (e.g.,802.11)
- ☐ Electronic data interchange (EDI)
- ☐ Internet
- ☐ Intranet
- ☐ Extranet
- ☐ Stand-alone PCs (not on LAN)
- ☐ Company-owned laptops
- ☐ Laptops not owned by company
- ☐ Other → Specify: _____

b. In 2005, what types of network access did this company support? *Mark ■ all that apply.*

- ☐ Hard-wired telecommunications lines
- ☐ Remote dial-in access via telecommunications lines
- ☐ Access to company networks or e-mail through Internet
- ☐ Wireless access to e-mail
- ☐ Wireless access to Internet
- ☐ Wireless access to this company's data or other networks
- ☐ Publicly accessible website WITHOUT e-commerce capabilities
- ☐ Publicly accessible website WITH e-commerce capabilities
- ☐ Other → Specify: _____

II. COMPUTER INFRASTRUCTURE & SECURITY - Continued

3a. In 2005, what types of computer system security technology did this company use? *Mark ■ all that apply.*

- ☐ Anti-virus software
- ☐ Anti-spyware/adware software
- ☐ Biometrics
- ☐ One-time password generators (smartcards, tokens, keys)
- ☐ Passwords that must be changed periodically
- ☐ Digital certificates
- ☐ Firewall
- ☐ DMZ Host
- ☐ Intrusion Detection System
- ☐ Intrusion Protection System
- ☐ E-mail logs or filters
- ☐ System administrative logs
- ☐ Encryption
- ☐ Other → Specify: _____

b. In 2005, how much did this company spend on the types of computer system security technology identified in 3a?
ESTIMATES are acceptable.
EXCLUDE personnel costs.

	Mil.			Thou.			Dol.		
$							0	0	0

c. What percentage of this company's total 2005 Information Technology budget did this company spend on the types of computer system security technology identified in 3a?
ESTIMATES are acceptable.
Round to nearest whole percent.

			%

d. What types of computer system security technology does this company plan to add in 2006?
EXCLUDE updates or upgrades of technologies already used in 2005.
Mark ■ all that apply.

- ☐ Anti-virus software
- ☐ Anti-spyware/adware software
- ☐ Biometrics
- ☐ One-time password generators (smartcards, tokens, keys)
- ☐ Passwords that must be changed periodically
- ☐ Digital certificates
- ☐ Firewall
- ☐ DMZ Host
- ☐ Intrusion Detection System
- ☐ Intrusion Protection System
- ☐ E-mail logs or filters
- ☐ System administrative logs
- ☐ Encryption
- ☐ Other → Specify: _____
- ☐ Do not plan to add any new technologies in 2006

4a. In 2005, what types of computer security practices did this company have? *Mark ■ all that apply.*

- ☐ Business continuity plan for computer systems
- ☐ Disaster recovery plan for computer systems
- ☐ Corporate policy on computer security
- ☐ Identification of company's critical assets
- ☐ Vulnerability/risk assessment
- ☐ Intrusion/penetration testing of computer security
- ☐ Computer/network watch center
- ☐ Configuration management
- ☐ Regular review of system/security administration logs
- ☐ Periodic computer security audits
- ☐ Formal computer security audit standards
- ☐ Physical/environmental security (e.g., limited physical access, sprinklers)
- ☐ Personnel policies (e.g., background checks, transfer, termination)
- ☐ Training employees in computer security practices
- ☐ Equipment decommissioning
- ☐ Other → Specify: _____

b. In 2005, what computer security functions did this company outsource? INCLUDE fully and/or partially outsourced functions.
Mark ■ all that apply.

- ☐ Business continuity plan for computer systems
- ☐ Disaster recovery plan for computer systems
- ☐ Corporate policy on computer security
- ☐ Identification of company's critical assets
- ☐ Vulnerability/risk assessment
- ☐ Intrusion/penetration testing of computer security
- ☐ Computer/network watch center
- ☐ Configuration management
- ☐ Regular review of system/security administration logs
- ☐ Periodic computer security audits
- ☐ Formal computer security audit standards
- ☐ Physical/environmental security (e.g., limited physical access, sprinklers)
- ☐ Personnel policies (e.g., background checks, transfer, termination)
- ☐ Training employees in computer security practices
- ☐ Equipment decommissioning
- ☐ Other → Specify: _____
- ☐ None; all computer security was done in-house

c. If this company had a computer system business continuity or disaster recovery plan, was it tested, used in an emergency situation and/or updated in 2005?
Mark ■ all that apply.

- ☐ Tested in 2005
- ☐ Used in emergency situation in 2005
- ☐ Updated in 2005
- ☐ Had plans but did not test, use, or update in 2005
- ☐ Other → Specify: _____
- ☐ Not applicable; did not have these plans in 2005

d. In 2005, how frequently did this company conduct formal vulnerability/risk assessments prior to implementing new applications, systems, or programs? *Mark ■ all that apply.*

- ☐ Always
- ☐ More than half the time
- ☐ Less than half the time
- ☐ When required by law
- ☐ Other → Specify: _____
- ☐ Never
- ☐ Did not implement any new applications, systems, or programs in 2005.

e. In 2005, did this company track downtime caused by any computer security incidents?

- ○ Yes
- ○ No

13532

III. TYPES OF COMPUTER SECURITY INCIDENTS

The questions in this section pertain to computer security incidents against this company, where the word "incident" refers to any unauthorized access, intrusion, breach, compromise or use of this company's computer system.

Computer security incidents may be committed by people either inside or outside the company and include computer virus, denial of service, vandalism, sabotage, embezzlement, fraud, theft of intellectual property, theft of personal or financial information, or other incidents such as hacking, spoofing, or spyware.

Please do NOT duplicate information. If an incident can be classified under multiple categories, report it under the FIRST applicable category. For example, if part of the company's computer system was deliberately damaged by means of a virus, report this under computer virus, not vandalism or sabotage.

ESTIMATES are acceptable.

5. COMPUTER VIRUS

A computer virus is a hidden fragment of computer code which propagates by inserting itself into or modifying other programs.

INCLUDE viruses, worms, Trojan horses, etc.

EXCLUDE spyware, adware, other malware, etc. Report these in 12 (Other Computer Security Incidents) on page 11.

a. In 2005, did this company intercept any computer viruses before they could infect any part of its computer systems?

- ◯ Yes
- ◯ No
- ◯ Don't know

b. Did this company detect any viruses which infected any part of its computer systems in 2005?

- ◯ Yes → **How many incidents were detected?** *If a virus simultaneously infects a server and one or more PCs, count this as ONE INCIDENT.* ☐☐☐☐☐☐ Number
- ◯ No → **(If "No", skip to 6.)**

c. Which of the following types of security technology or practices were inadequate in preventing these incidents? *Mark ■ all that apply.*

- ☐ Internal computer security controls
- ☐ External computer security controls
- ☐ Anti-Virus software
- ☐ Anti-spyware/adware software
- ☐ Biometrics
- ☐ One-time password generators
- ☐ Passwords that must be changed
- ☐ Digital certificates
- ☐ Firewall
- ☐ DMZ Host
- ☐ Intrusion Detection System
- ☐ Intrusion Protection System
- ☐ Encryption
- ☐ Software vulnerability/buffer overload
- ☐ E-mail filters or review of e-mail logs
- ☐ Review of system/security admin logs
- ☐ Computer network/watch center
- ☐ Configuration management
- ☐ Physical/environmental security
- ☐ Personnel policies
- ☐ Authorized access misused
- ☐ Other → Specify: _____
- ☐ Don't know

d. Through which of the following were the viruses introduced into this company's networks in these incidents? *Mark ■ all that apply.*

- ☐ E-mail attachments
- ☐ Software installation
- ☐ Files brought in on portable media such as floppy disks, CDs, or flash drives
- ☐ Files downloaded from the Internet
- ☐ Other → Specify: _____
- ☐ Don't know

e. To which of the following organizations were these incidents reported? *Mark ■ all that apply.*

- ☐ Local law enforcement
- ☐ State law enforcement
- ☐ FBI (Federal Bureau of Investigation)
- ☐ US-CERT (United States Computer Emergency Readiness Team)
- ☐ Other Federal agency → Specify: _____
- ☐ CERT® Coordination Center
- ☐ ISAC (Information Sharing and Analysis Center)
- ☐ InfraGard
- ☐ None of the above

f. How many of these incidents were reported to the organizations specified in 5e? ☐☐☐☐☐☐ Number

g. If any incidents were not reported to the organizations specified in 5e, what were the reasons? *Mark ■ all that apply.*

- ☐ Handled internally
- ☐ Reported to third party contractor providing computer security services
- ☐ Reported to another organization → Specify: _____
- ☐ Negative publicity
- ☐ Lower customer/client/investor confidence
- ☐ Competitor advantage
- ☐ Did not want data/hardware seized as evidence
- ☐ Did not know who to contact
- ☐ Incident outside jurisdiction of law enforcement
- ☐ Did not think to report
- ☐ Nothing to be gained/nothing worth pursuing
- ☐ Other → Specify: _____

III. TYPES OF COMPUTER SECURITY INCIDENTS – Continued

h. What was the relationship between the suspected offender (the person who sent or created the virus) and this company at the time of the incidents indicated in 5b? *Mark ■ all that apply.*

- ☐ Insider - someone currently (or formerly) working for this company
- ☐ Current employee
- ☐ Current contractor, vendor, temporary worker, etc.
- ☐ Former employee, contractor, vendor, temporary worker, etc.
- ☐ Outsider - someone who never worked for this company
- ☐ Domestic competitor
- ☐ Foreign competitor → Specify country: _____
- ☐ Domestic hacker
- ☐ Foreign hacker → Specify country: _____
- ☐ Other hacker (origin unknown)
- ☐ Other → Specify: _____
- ☐ Don't know

i. What was the total downtime (in hours) for each of the following due to these virus infections? ESTIMATES are acceptable.

INCLUDE downtime needed for repair.

1. Downtime of servers, routers or switches Hours | | | | | | |

2. Downtime of individual PCs/workstations Hours | | | | | | |
EXCLUDE network downtime reported above in item i,1.

j. How much was spent in 2005 to recover from these computer viruses? ESTIMATES are acceptable.

INCLUDE the cost - both internal and external - of diagnosis, repair, and replacement such as labor, hardware, software, etc.
EXCLUDE costs associated solely with the prevention of future incidents.

	Mil.			Thou.			Dol.
$							0 0 0

k. What other monetary losses and costs were incurred in 2005 due to these incidents? ESTIMATES are acceptable.

INCLUDE actual losses such as the value of lost information.
INCLUDE the estimated value of downtime, lost productivity, income from lost sales, labor or fees for legal or investigative work, etc.

	Mil.			Thou.			Dol.
$							0 0 0

III. TYPES OF COMPUTER SECURITY INCIDENTS – Continued

6. DENIAL OF SERVICE

Denial of service is the disruption, degradation, or exhaustion of an Internet connection or e-mail service that results in an interruption of the normal flow of information. Denial of service is usually caused by ping attacks, port scanning probes, excessive amounts of incoming data, etc.

EXCLUDE incidents already reported under 5 (Computer Virus) on page 3.

a. Did this company detect any incidents of denial of service (a noticeable interruption of its Internet connection or e-mail service) in 2005?

○ Yes → **How many incidents were detected?** ☐☐☐☐☐☐ Number

○ No → **(If "No", skip to 7.)**

b. Which of the following types of security technology or practices were inadequate in preventing these incidents? *Mark ■ all that apply.*

- ☐ Internal computer security controls
- ☐ External computer security controls
- ☐ Anti-virus software
- ☐ Anti-spyware/adware software
- ☐ Biometrics
- ☐ One-time password generators
- ☐ Passwords that must be changed
- ☐ Digital certificates
- ☐ Firewall
- ☐ DMZ Host
- ☐ Intrusion Detection System
- ☐ Intrusion Protection System
- ☐ Encryption
- ☐ Software vulnerability/buffer overload
- ☐ E-mail filters or review of e-mail logs
- ☐ Review of system/security admin logs
- ☐ Computer network/watch center
- ☐ Configuration management
- ☐ Physical/environmental security
- ☐ Personnel policies
- ☐ Authorized access misused
- ☐ Other → Specify: _____
- ☐ Don't know

c. Which of the following were used, accessed, or affected in these incidents? *Mark ■ all that apply.*

- ☐ Local area network (LAN)
- ☐ Wide area network (WAN)
- ☐ Process control network (PCN)
- ☐ Virtual private network (VPN)
- ☐ Wireless network (e.g.,802.11)
- ☐ Electronic data interchange (EDI)
- ☐ Internet
- ☐ Intranet
- ☐ Extranet
- ☐ Stand-alone PCs (not on LAN)
- ☐ Company-owned laptop
- ☐ Laptop not owned by company
- ☐ Other → Specify: _____
- ☐ Don't know

d. To which of the following organizations were these incidents reported? *Mark ■ all that apply.*

- ☐ Local law enforcement
- ☐ State law enforcement
- ☐ FBI (Federal Bureau of Investigation)
- ☐ US-CERT (United States Computer Emergency Readiness Team)
- ☐ Other Federal agency → Specify: _____
- ☐ CERT® Coordination Center
- ☐ ISAC (Information Sharing and Analysis Center)
- ☐ InfraGard
- ☐ None of the above

e. How many of these incidents were reported to the organizations specified in 6d? ☐☐☐☐☐☐ Number

f. If any incidents were not reported to the organizations specified in 6d, what were the reasons? *Mark ■ all that apply.*

- ☐ Handled internally
- ☐ Reported to third party contractor providing computer security services
- ☐ Reported to another organization → Specify: _____
- ☐ Negative publicity
- ☐ Lower customer/client/investor confidence
- ☐ Competitor advantage
- ☐ Did not want data/hardware seized as evidence
- ☐ Did not know who to contact
- ☐ Incident outside jurisdiction of law enforcement
- ☐ Did not think to report
- ☐ Nothing to be gained/nothing worth pursuing
- ☐ Other → Specify: _____

g. What was the relationship between the suspected offender and this company at the time of the incidents indicated in 6a? *Mark ■ all that apply.*

- ☐ Insider - someone currently (or formerly) working for this company
- ☐ Current employee
- ☐ Current contractor, vendor, temporary worker, etc.
- ☐ Former employee, contractor, vendor, temporary worker, etc.
- ☐ Outsider - someone who never worked for this company
- ☐ Domestic competitor
- ☐ Foreign competitor → Specify country: _____
- ☐ Domestic hacker
- ☐ Foreign hacker → Specify country: _____
- ☐ Other hacker (origin unknown)
- ☐ Other → Specify: _____
- ☐ Don't know

h. What was the total duration (in hours) of the incidents of denial of service indicated in 6a? ESTIMATES are acceptable. INCLUDE downtime needed for repairs. Hours ☐☐☐☐☐☐

i. How much was spent in 2005 to recover from these incidents of denial of service? ESTIMATES are acceptable. INCLUDE the cost - both internal and external - of diagnosis, repair, and replacement such as labor, hardware, software, etc. EXCLUDE costs associated solely with the prevention of future incidents.

	Mil.	Thou.	Dol.
$	☐☐☐	☐☐☐	000

j. What other monetary losses and costs were incurred in 2005 due to these incidents? ESTIMATES are acceptable. INCLUDE the estimated value of downtime, lost productivity, income from lost sales, labor or fees for legal or investigative work, etc.

	Mil.	Thou.	Dol.
$	☐☐☐	☐☐☐	000

III. TYPES OF COMPUTER SECURITY INCIDENTS – Continued

7. ELECTRONIC VANDALISM OR SABOTAGE

Electronic vandalism or sabotage is the deliberate or malicious damage, defacement, destruction or other alteration of electronic files, data, web pages, programs, etc.

EXCLUDE incidents already reported under 5 (Computer Virus) on page 3.

EXCLUDE incidents of alteration which resulted in fraud. Report these in 9 (Fraud) on page 8.

a. Did this company detect any incidents in which files, data, web pages or any part of its computer systems were electronically vandalized or sabotaged in 2005?

○ Yes → **How many incidents were detected?** Number

○ No → **(If "No", skip to 8.)**

b. Which of the following types of security technology or practices were inadequate in preventing these incidents? *Mark ■ all that apply.*

- ☐ Internal computer security controls
- ☐ External computer security controls
- ☐ Anti-virus software
- ☐ Anti-spyware/adware software
- ☐ Biometrics
- ☐ One-time password generators
- ☐ Passwords that must be changed
- ☐ Digital certificates
- ☐ Firewall
- ☐ DMZ Host
- ☐ Intrusion Detection System
- ☐ Intrusion Protection System
- ☐ Encryption
- ☐ Software vulnerability/buffer overload
- ☐ E-mail filters or review of e-mail logs
- ☐ Review of system/security admin logs
- ☐ Computer network/watch center
- ☐ Configuration management
- ☐ Physical/environmental security
- ☐ Personnel policies
- ☐ Authorized access misused
- ☐ Other → Specify: _____
- ☐ Don't know

c. Which of the following were used, accessed, or affected in these incidents? *Mark ■ all that apply.*

- ☐ Local area network (LAN)
- ☐ Wide area network (WAN)
- ☐ Process control network (PCN)
- ☐ Virtual private network (VPN)
- ☐ Wireless network (e.g.,802.11)
- ☐ Electronic data interchange (EDI)
- ☐ Internet
- ☐ Intranet
- ☐ Extranet
- ☐ Stand-alone PCs (not on LAN)
- ☐ Company-owned laptop
- ☐ Laptop not owned by company
- ☐ Other → Specify: _____
- ☐ Don't know

d. To which of the following organizations were these incidents reported? *Mark ■ all that apply.*

- ☐ Local law enforcement
- ☐ State law enforcement
- ☐ FBI (Federal Bureau of Investigation)
- ☐ US-CERT (United States Computer Emergency Readiness Team)
- ☐ Other Federal agency → Specify: _____
- ☐ CERT® Coordination Center
- ☐ ISAC (Information Sharing and Analysis Center)
- ☐ InfraGard
- ☐ None of the above

e. How many of these incidents were reported to the organizations specified in 7d? Number

f. If any incidents were not reported to the organizations listed in 7d, what were the reasons? *Mark ■ all that apply.*

- ☐ Handled internally
- ☐ Reported to third party contractor providing computer security services
- ☐ Reported to another organization → Specify: _____
- ☐ Negative publicity
- ☐ Lower customer/client/investor confidence
- ☐ Competitor advantage
- ☐ Did not want data/hardware seized as evidence
- ☐ Did not know who to contact
- ☐ Incident outside jurisdiction of law enforcement
- ☐ Did not think to report
- ☐ Nothing to be gained/nothing worth pursuing
- ☐ Other → Specify: _____

g. What was the relationship between the suspected offender and this company at the time of the incidents indicated in 7a? *Mark ■ all that apply.*

- ☐ Insider - someone currently (or formerly) working for this company
- ☐ Current employee
- ☐ Current contractor, vendor, temporary worker, etc.
- ☐ Former employee, contractor, vendor, temporary worker, etc.
- ☐ Outsider - someone who never worked for this company
- ☐ Domestic competitor
- ☐ Foreign competitor → Specify country: _____
- ☐ Domestic hacker
- ☐ Foreign hacker → Specify country: _____
- ☐ Other hacker (origin unknown)
- ☐ Other → Specify: _____
- ☐ Don't know

h. What was the total downtime (in hours) of each of the following due to these acts of vandalism or sabotage? ESTIMATES are acceptable.

INCLUDE downtime needed for repair.

1. Downtime of company websites/ web servers	Hours
2. Downtime of servers, routers or switches EXCLUDE downtime reported above in item h,1.	Hours
3. Downtime of individual PCs/workstations EXCLUDE downtime reported above in item h,1 or 2.	Hours

i. How much was spent in 2005 to recover from these incidents of vandalism or sabotage? ESTIMATES are acceptable. INCLUDE the cost - both internal and external - of diagnosis, repair, and replacement such as labor, hardware, software, etc. EXCLUDE costs associated solely with the prevention of future incidents.

	Mil.	Thou.	Dol.
$			000

j. What other monetary losses and costs were incurred in 2005 due to these incidents? ESTIMATES are acceptable. INCLUDE actual losses such as the value of lost information. INCLUDE the estimated value of downtime, lost productivity, income from lost sales, labor or fees for legal or investigative work, etc.

	Mil.	Thou.	Dol.
$			000

13532

III. TYPES OF COMPUTER SECURITY INCIDENTS – Continued

8. EMBEZZLEMENT

Embezzlement is the unlawful misappropriation of money or other things of value, BY THE PERSON TO WHOM IT WAS ENTRUSTED (typically an employee), for his/her own use or purpose.

INCLUDE instances in which a computer was used to wrongfully transfer, counterfeit, forge or gain access to money, property, financial documents, insurance policies, deeds, use of rental cars, various services, etc., by the person to whom it was entrusted.

a. Did this company detect any incidents in which a computer was used to commit embezzlement against this company in 2005?

○ Yes → **How many incidents were detected?** [ ][ ][ ][ ][ ][ ] Number

○ No → **(If "No", skip to 9.)**

b. Which of the following types of security technology or practices were inadequate in preventing these incidents? *Mark ■ all that apply.*

- ☐ Internal computer security controls
- ☐ External computer security controls
- ☐ Anti-virus software
- ☐ Anti-spyware/adware software
- ☐ Biometrics
- ☐ One-time password generators
- ☐ Passwords that must be changed
- ☐ Digital certificates
- ☐ Firewall
- ☐ DMZ Host
- ☐ Intrusion Detection System
- ☐ Intrusion Protection System
- ☐ Encryption
- ☐ Software vulnerability/buffer overload
- ☐ E-mail filters or review of e-mail logs
- ☐ Review of system/security admin logs
- ☐ Computer network/watch center
- ☐ Configuration management
- ☐ Physical/environmental security
- ☐ Personnel policies
- ☐ Authorized access misused
- ☐ Other → Specify: _____
- ☐ Don't know

c. Which of the following were used, accessed, or affected in these incidents? *Mark ■ all that apply.*

- ☐ Local area network (LAN)
- ☐ Wide area network (WAN)
- ☐ Process control network (PCN)
- ☐ Virtual private network (VPN)
- ☐ Wireless network (e.g.,802.11)
- ☐ Electronic data interchange (EDI)
- ☐ Internet
- ☐ Intranet
- ☐ Extranet
- ☐ Stand-alone PCs (not on LAN)
- ☐ Company-owned laptop
- ☐ Laptop not owned by company
- ☐ Other → Specify: _____
- ☐ Don't know

d. To which of the following official organizations were these incidents reported? *Mark ■ all that apply.*

- ☐ Local law enforcement
- ☐ State law enforcement
- ☐ FBI (Federal Bureau of Investigation)
- ☐ US-CERT (United States Computer Emergency Readiness Team)
- ☐ Other Federal agency → Specify: _____
- ☐ CERT® Coordination Center
- ☐ ISAC (Information Sharing and Analysis Center)
- ☐ InfraGard
- ☐ None of the above

e. How many of these incidents were reported to the organizations specified in 8d? [ ][ ][ ][ ][ ][ ] Number

f. If any incidents were not reported to the organizations specified in 8d, what were the reasons? *Mark ■ all that apply.*

- ☐ Handled internally
- ☐ Reported to third party contractor providing computer security services
- ☐ Reported to another organization → Specify: _____
- ☐ Negative publicity
- ☐ Lower customer/client/investor confidence
- ☐ Competitor advantage
- ☐ Did not want data/hardware seized as evidence
- ☐ Did not know who to contact
- ☐ Incident outside jurisdiction of law enforcement
- ☐ Did not think to report
- ☐ Nothing to be gained/nothing worth pursuing
- ☐ Other → Specify: _____

g. What was the relationship between the suspected offender and this company at the time of the incidents indicated in 8a? *Mark ■ all that apply.*

- ☐ Insider - someone currently (or formerly) working for this company
- ☐ Current employee
- ☐ Current contractor, vendor, temporary worker, etc.
- ☐ Former employee, contractor, vendor, temporary worker, etc.
- ☐ Outsider - someone who never worked for this company
- ☐ Domestic competitor
- ☐ Foreign competitor → Specify country: _____
- ☐ Domestic hacker
- ☐ Foreign hacker → Specify country: _____
- ☐ Other hacker (origin unknown)
- ☐ Other → Specify: _____
- ☐ Don't know

h. What was the dollar value of money or other things taken by embezzlement in 2005? ESTIMATES are acceptable.

	Mil.	Thou.	Dol.
$	[ ][ ][ ]	[ ][ ][ ]	000

i. What other monetary losses and costs were incurred in 2005 due to these incidents? ESTIMATES are acceptable.
INCLUDE the cost of diagnosis, repair and replacement such as labor, hardware, software, etc. If possible, include the estimated value of downtime, lost productivity, income from lost sales, labor or fees for legal or investigative work, etc.
EXCLUDE costs associated solely with the prevention of future incidents.

	Mil.	Thou.	Dol.
$	[ ][ ][ ]	[ ][ ][ ]	000

III. TYPES OF COMPUTER SECURITY INCIDENTS – Continued

9. FRAUD

Fraud is the intentional misrepresentation of information or identity to deceive others, the unlawful use of credit/debit card or ATM or the use of electronic means to transmit deceptive information, in order to obtain money or other things of value. Fraud may be committed by someone inside or outside the company.

INCLUDE instances in which a computer was used by someone inside or outside this company in order to defraud this company of money, property, financial documents, insurance policies, deeds, use of rental cars, various services, etc., by means of forgery, misrepresented identity, credit card or wire fraud, etc.

EXCLUDE incidents of embezzlement. Report these in 8 (Embezzlement) on page 7.

a. Did this company detect any incidents in which someone inside or outside this company used a computer to commit fraud against this company in 2005?

○ Yes → **How many incidents were detected?** ☐☐☐☐☐☐ Number

○ No → **(If "No", skip to 10.)**

b. Which of the following types of security technology or practices were inadequate in preventing these incidents? *Mark ■ all that apply.*

- ☐ Internal computer security controls
- ☐ External computer security controls
- ☐ Anti-virus software
- ☐ Anti-spyware/adware software
- ☐ Biometrics
- ☐ One-time password generators
- ☐ Passwords that must be changed
- ☐ Digital certificates
- ☐ Firewall
- ☐ DMZ Host
- ☐ Intrusion Detection System
- ☐ Intrusion Protection System
- ☐ Encryption
- ☐ Software vulnerability/buffer overload
- ☐ E-mail filters or review of e-mail logs
- ☐ Review of system/security admin logs
- ☐ Computer network/watch center
- ☐ Configuration management
- ☐ Physical/environmental security
- ☐ Personnel policies
- ☐ Authorized access misused
- ☐ Other → Specify: _____
- ☐ Don't know

c. Which of the following were used, accessed, or affected in these incidents? *Mark ■ all that apply.*

- ☐ Local area network (LAN)
- ☐ Wide area network (WAN)
- ☐ Process control network (PCN)
- ☐ Virtual private network (VPN)
- ☐ Wireless network (e.g.,802.11)
- ☐ Electronic data interchange (EDI)
- ☐ Internet
- ☐ Intranet
- ☐ Extranet
- ☐ Stand-alone PCs (not on LAN)
- ☐ Company-owned laptop
- ☐ Laptop not owned by company
- ☐ Other → Specify: _____
- ☐ Don't know

d. To which of the following organizations were these incidents reported? *Mark ■ all that apply.*

- ☐ Local law enforcement
- ☐ State law enforcement
- ☐ FBI (Federal Bureau of Investigation)
- ☐ US-CERT (United States Computer Emergency Readiness Team)
- ☐ Other Federal agency → Specify: _____
- ☐ CERT® Coordination Center
- ☐ ISAC (Information Sharing and Analysis Center)
- ☐ InfraGard
- ☐ None of the above

e. How many of these incidents were reported to the organizations specified in 9d? ☐☐☐☐☐☐ Number

f. If any incidents were not reported to the organizations specified in 9d, what were the reasons? *Mark ■ all that apply.*

- ☐ Handled internally
- ☐ Reported to third party contractor providing computer security services
- ☐ Reported to another organization → Specify: _____
- ☐ Negative publicity
- ☐ Lower customer/client/investor confidence
- ☐ Competitor advantage
- ☐ Did not want data/hardware seized as evidence
- ☐ Did not know who to contact
- ☐ Incident outside jurisdiction of law enforcement
- ☐ Did not think to report
- ☐ Nothing to be gained/nothing worth pursuing
- ☐ Other → Specify: _____

g. What was the relationship between the suspected offender and this company at the time of the incidents indicated in 9a? *Mark ■ all that apply.*

- ☐ Insider - someone currently (or formerly) working for this company
- ☐ Current employee
- ☐ Current contractor, vendor, temporary worker, etc.
- ☐ Former employee, contractor, vendor, temporary worker, etc.
- ☐ Outsider - someone who never worked for this company
- ☐ Domestic competitor
- ☐ Foreign competitor → Specify country: _____
- ☐ Domestic hacker
- ☐ Foreign hacker → Specify country: _____
- ☐ Other hacker (origin unknown)
- ☐ Other → Specify: _____
- ☐ Don't know

h. What was the dollar value of money or other things taken by fraud in 2005? ESTIMATES are acceptable.

	Mil.	Thou.	Dol.
$			000

i. What other monetary losses and costs were incurred in 2005 due to these incidents? ESTIMATES are acceptable. INCLUDE the cost of diagnosis, repair and replacement such as labor, hardware, software, etc. If possible, include the estimated value of downtime, lost productivity, income from lost sales, labor or fees for legal or investigative work, etc. EXCLUDE costs associated solely with the prevention of future incidents.

	Mil.	Thou.	Dol.
$			000

13532

III. TYPES OF COMPUTER SECURITY INCIDENTS – Continued

10. THEFT OF INTELLECTUAL PROPERTY

Theft of intellectual property is the illegal obtaining of copyrighted or patented material, trade secrets, or trademarks including designs, plans, blueprints, codes, computer programs, software, formulas, recipes, graphics, etc., usually by electronic copying.

EXCLUDE incidents of theft of personal or financial data such as credit card or social security numbers, names and dates of birth, financial account information, etc. Report these in 11 (Theft of Personal or Financial Data) on page 10.

EXCLUDE incidents of theft of any other type of information. Report these in 12 (Other Computer Security Incidents) on page 11.

a. Did this company detect any incidents in which someone inside or outside this company used a computer to obtain intellectual property from this company in 2005?

○ Yes → **How many incidents were detected?** ☐☐☐☐☐☐ Number

○ No → **(If "No", skip to 11.)**

b. What type of intellectual property was obtained? *Mark ■ all that apply.*

- ☐ Copyrighted material
- ☐ Patented material
- ☐ Trade secrets
- ☐ Trademarks

c. Which of the following types of security technology or practices were inadequate in preventing these incidents? *Mark ■ all that apply.*

- ☐ Internal computer security controls
- ☐ External computer security controls
- ☐ Anti-virus software
- ☐ Anti-spyware/adware software
- ☐ Biometrics
- ☐ One-time password generators
- ☐ Passwords that must be changed
- ☐ Digital certificates
- ☐ Firewall
- ☐ DMZ Host
- ☐ Intrusion Detection System
- ☐ Intrusion Protection System
- ☐ Encryption
- ☐ Software vulnerability/buffer overload
- ☐ E-mail filters or review of e-mail logs
- ☐ Review of system/security admin logs
- ☐ Computer network/watch center
- ☐ Configuration management
- ☐ Physical/environmental security
- ☐ Personnel policies
- ☐ Authorized access misused
- ☐ Other → Specify: _____
- ☐ Don't know

d. Which of the following were used, accessed, or affected in these incidents? *Mark ■ all that apply.*

- ☐ Local area network (LAN)
- ☐ Wide area network (WAN)
- ☐ Process control network (PCN)
- ☐ Virtual private network (VPN)
- ☐ Wireless network (e.g.,802.11)
- ☐ Electronic data interchange (EDI)
- ☐ Internet
- ☐ Intranet
- ☐ Extranet
- ☐ Stand-alone PCs (not on LAN)
- ☐ Company-owned laptop
- ☐ Laptop not owned by company
- ☐ Other → Specify: _____
- ☐ Don't know

e. To which of the following organizations were these incidents reported? *Mark ■ all that apply.*

- ☐ Local law enforcement
- ☐ State law enforcement
- ☐ FBI (Federal Bureau of Investigation)
- ☐ US-CERT (United States Computer Emergency Readiness Team)
- ☐ Other Federal agency → Specify: _____
- ☐ CERT® Coordination Center
- ☐ ISAC (Information Sharing and Analysis Center)
- ☐ InfraGard
- ☐ None of the above

f. How many of these incidents were reported to the organizations specified in 10e? ☐☐☐☐☐☐ Number

g. If any incidents were not reported to the organizations specified in 10e, what were the reasons? *Mark ■ all that apply.*

- ☐ Handled internally
- ☐ Reported to third party contractor providing computer security services
- ☐ Reported to another organization → Specify: _____
- ☐ Negative publicity
- ☐ Lower customer/client/investor confidence
- ☐ Competitor advantage
- ☐ Did not want data/hardware seized as evidence
- ☐ Did not know who to contact
- ☐ Incident outside jurisdiction of law enforcement
- ☐ Did not think to report
- ☐ Nothing to be gained/nothing worth pursuing
- ☐ Other → Specify: _____

h. What was the relationship between the suspected offender and this company at the time of the incidents indicated in 10a? *Mark ■ all that apply.*

- ☐ Insider - someone currently (or formerly) working for this company
- ☐ Current employee
- ☐ Current contractor, vendor, temporary worker, etc.
- ☐ Former employee, contractor, vendor, temporary worker, etc.
- ☐ Outsider - someone who never worked for this company
- ☐ Domestic competitor
- ☐ Foreign competitor → Specify country: _____
- ☐ Domestic hacker
- ☐ Foreign hacker → Specify country: _____
- ☐ Other hacker (origin unknown)
- ☐ Other → Specify: _____
- ☐ Don't know

i. What was the dollar value of intellectual property taken by theft in 2005? ESTIMATES are acceptable.

	Mil.	Thou.	Dol.
$			000

j. What other monetary losses and costs were incurred in 2005 due to these incidents? ESTIMATES are acceptable. INCLUDE the cost of diagnosis, repair and replacement such as labor, hardware, software, etc. If possible, include the estimated value of downtime, lost productivity, income from lost sales, labor or fees for legal or investigative work, etc. EXCLUDE costs associated solely with the prevention of future incidents.

	Mil.	Thou.	Dol.
$			000

k. How many of the incidents indicated in 10a involved unlicensed use or copying (piracy) of digital products which this company developed for resale? ☐☐☐☐☐☐ Number

III. TYPES OF COMPUTER SECURITY INCIDENTS – Continued

11. THEFT OF PERSONAL OR FINANCIAL INFORMATION

Theft of personal or financial information is the illegal obtaining of information that could potentially allow someone to use or create accounts under another name (individual, business, or some other entity). Personal information includes names, dates of birth, social security numbers, etc. Financial information includes credit/debit/ATM card, account, or PIN numbers, etc.

EXCLUDE incidents of theft of intellectual property such as copyrights, patents, trade secrets, and trademarks. Report these in 10 (Theft of Intellectual Property) on page 9.

EXCLUDE incidents of theft of any other type of information. Report these in 12 (Other Computer Security Incidents) on page 11.

a. Did this company detect any incidents in which someone inside or outside this company used a computer to obtain personal or financial information from this company in 2005?

○ Yes → **How many incidents were detected?** ☐☐☐☐☐☐ Number

○ No → **(If "No", skip to 12.)**

b. What type of personal or financial information was obtained? *Mark ■ all that apply.*

- ☐ Names or dates of birth
- ☐ Social security numbers
- ☐ Credit card numbers
- ☐ Debit or ATM card numbers
- ☐ Account or PIN numbers
- ☐ Other → Specify: _____

c. Which of the following types of security technology or practices were inadequate in preventing these incidents? *Mark ■ all that apply.*

- ☐ Internal computer security controls
- ☐ External computer security controls
- ☐ Anti-virus software
- ☐ Anti-spyware/adware software
- ☐ Biometrics
- ☐ One-time password generators
- ☐ Passwords that must be changed
- ☐ Digital certificates
- ☐ Firewall
- ☐ DMZ Host
- ☐ Intrusion Detection System
- ☐ Intrusion Protection System
- ☐ Encryption
- ☐ Software vulnerability/buffer overload
- ☐ E-mail filters or review of e-mail logs
- ☐ Review of system/security admin logs
- ☐ Computer network/watch center
- ☐ Configuration management
- ☐ Physical/environmental security
- ☐ Personnel policies
- ☐ Authorized access misused
- ☐ Other → Specify: _____
- ☐ Don't know

d. Which of the following were used, accessed, or affected in these incidents? *Mark ■ all that apply.*

- ☐ Local area network (LAN)
- ☐ Wide area network (WAN)
- ☐ Process control network (PCN)
- ☐ Virtual private network (VPN)
- ☐ Wireless network (e.g.,802.11)
- ☐ Electronic data interchange (EDI)
- ☐ Internet
- ☐ Intranet
- ☐ Extranet
- ☐ Stand-alone PCs (not on LAN)
- ☐ Company-owned laptop
- ☐ Laptop not owned by company
- ☐ Other → Specify: _____
- ☐ Don't know

e. To which of the following organizations were these incidents reported? *Mark ■ all that apply.*

- ☐ Local law enforcement
- ☐ State law enforcement
- ☐ FBI (Federal Bureau of Investigation) Emergency Readiness Team)
- ☐ US-CERT (United States Computer
- ☐ Other Federal agency → Specify: _____
- ☐ CERT® Coordination Center
- ☐ ISAC (Information Sharing and Analysis Center)
- ☐ InfraGard
- ☐ None of the above

f. How many of these incidents were reported to the organizations specified in 11e? ☐☐☐☐☐☐ Number

g. If any incidents were not reported to the organizations specified in 11e, what were the reasons? *Mark ■ all that apply.*

- ☐ Handled internally
- ☐ Reported to third party contractor providing computer security services
- ☐ Reported to another organization →Specify: _____
- ☐ Negative publicity
- ☐ Lower customer/client/investor confidence
- ☐ Competitor advantage
- ☐ Did not want data/hardware seized as evidence
- ☐ Did not know who to contact
- ☐ Incident outside jurisdiction of law enforcement
- ☐ Did not think to report
- ☐ Nothing to be gained/nothing worth pursuing
- ☐ Other →Specify: _____

h. What was the relationship between the suspected offender and this company at the time of the incidents indicated in 11a? *Mark ■ all that apply.*

- ☐ Insider - someone currently (or formerly) working for this company
- ☐ Current employee
- ☐ Current contractor, vendor, temporary worker, etc.
- ☐ Former employee, contractor, vendor, temporary worker, etc.
- ☐ Outsider - someone who never worked for this company
- ☐ Domestic competitor
- ☐ Foreign competitor → Specify country: _____
- ☐ Domestic hacker
- ☐ Foreign hacker → Specify country: _____
- ☐ Other hacker (origin unknown)
- ☐ Other → Specify: _____
- ☐ Don't know

i. What was the dollar value of personal or financial information taken by theft in 2005? ESTIMATES are acceptable.

	Mil.	Thou.	Dol.
$			000

j. What other monetary losses and costs were incurred in 2005 due to these incidents? ESTIMATES are acceptable. INCLUDE the cost of diagnosis, repair and replacement such as labor, hardware, software, etc. If possible, include the estimated value of downtime, lost productivity, income from lost sales, labor or fees for legal or investigative work, etc. EXCLUDE costs associated solely with the prevention of future incidents.

	Mil.	Thou.	Dol.
$			000

13532

III. TYPES OF COMPUTER SECURITY INCIDENTS – Continued

12. OTHER COMPUTER SECURITY INCIDENTS

INCLUDE all other computer security incidents involving this company's computer networks—such as hacking, sniffing, spyware, theft of other information—regardless of whether damage or losses were sustained as a result.

EXCLUDE incidents already reported in this survey.

a. Did this company detect any other computer security incidents in 2005?

○ Yes → **How many incidents were detected?** ☐☐☐☐☐☐ Number

○ No → **(If "No", skip to 13.)**

b. What other types of computer security incidents were detected in 2005? *Mark ■ all that apply.*

- ☐ Hacking
- ☐ Spoofing
- ☐ Phishing
- ☐ Sniffing
- ☐ Pinging
- ☐ Scanning
- ☐ Spyware, keystroke logging
- ☐ Adware
- ☐ Other malware
- ☐ Theft of information not already reported in 10 or 11 on pages 8 or 9 → Please describe: _____
- ☐ Other → Please describe: _____

c. Which of the following types of security technology or practices were inadequate in preventing these incidents? *Mark ■ all that apply.*

- ☐ Internal computer security controls
- ☐ External computer security controls
- ☐ Anti-virus software
- ☐ Anti-spyware/adware software
- ☐ Biometrics
- ☐ One-time password generators
- ☐ Passwords that must be changed
- ☐ Digital certificates
- ☐ Firewall
- ☐ DMZ Host
- ☐ Intrusion Detection System
- ☐ Intrusion Protection System
- ☐ Encryption
- ☐ Software vulnerability/buffer overload
- ☐ E-mail filters or review of e-mail logs
- ☐ Review of system/security admin logs
- ☐ Computer network/watch center
- ☐ Configuration management
- ☐ Physical/environmental security
- ☐ Personnel policies
- ☐ Authorized access misused
- ☐ Other → Specify: _____
- ☐ Don't know

d. Which of the following were used, accessed, or affected in these incidents? *Mark ■ all that apply.*

- ☐ Local area network (LAN)
- ☐ Wide area network (WAN)
- ☐ Process control network (PCN)
- ☐ Virtual private network (VPN)
- ☐ Wireless network (e.g.,802.11)
- ☐ Electronic data interchange (EDI)
- ☐ Internet
- ☐ Intranet
- ☐ Extranet
- ☐ Stand-alone PCs (not on LAN)
- ☐ Company-owned laptop
- ☐ Laptop not owned by company
- ☐ Other → Specify: _____
- ☐ Don't know

e. To which of the following organizations were these incidents reported? *Mark ■ all that apply.*

- ☐ Local law enforcement
- ☐ State law enforcement
- ☐ FBI (Federal Bureau of Investigation)
- ☐ US-CERT (United States Computer Emergency Readiness Team)
- ☐ Other Federal agency → Specify: _____
- ☐ CERT® Coordination Center
- ☐ ISAC (Information Sharing and Analysis Center)
- ☐ InfraGard
- ☐ None of the above

f. How many of these incidents were reported to the organizations specified in 12e? ☐☐☐☐☐☐ Number

g. If any incidents were not reported to the organizations listed in 12e, what were the reasons? *Mark ■ all that apply.*

- ☐ Handled internally
- ☐ Reported to third party contractor providing computer security services
- ☐ Reported to another organization → Specify: _____
- ☐ Negative publicity
- ☐ Lower customer/client/investor confidence
- ☐ Competitor advantage
- ☐ Did not want data/hardware seized as evidence
- ☐ Did not know who to contact
- ☐ Incident outside jurisdiction of law enforcement
- ☐ Did not think to report
- ☐ Nothing to be gained/nothing worth pursuing
- ☐ Other → Specify: _____

h. What was the relationship between the suspected offender and this company at the time of the incidents indicated in 12a? *Mark ■ all that apply.*

- ☐ Insider - someone currently (or formerly) working for this company
- ☐ Current employee
- ☐ Current contractor, vendor, temporary worker, etc.
- ☐ Former employee, contractor, vendor, temporary worker, etc.
- ☐ Outsider - someone who never worked for this company
- ☐ Domestic competitor
- ☐ Foreign competitor → Specify country: _____
- ☐ Domestic hacker
- ☐ Foreign hacker → Specify country: _____
- ☐ Other hacker (origin unknown)
- ☐ Other → Specify: _____
- ☐ Don't know

i. If any, what was the total downtime (in hours) of each of the following due to these other computer security incidents? ESTIMATES are acceptable.

INCLUDE downtime needed for repair.

1. Downtime of company websites/ web servers	Hours	☐☐☐☐☐☐
2. Downtime of servers, routers or switches EXCLUDE downtime reported above in item i,1.	Hours	☐☐☐☐☐☐
3. Downtime of individual PCs/workstations EXCLUDE downtime reported above in item i,1 or 2.	Hours	☐☐☐☐☐☐

j. How much was spent in 2005 to recover from these other computer security incidents? ESTIMATES are acceptable. INCLUDE the cost - both internal and external - of diagnosis, repair, and replacement such as labor, hardware, software, etc. EXCLUDE costs associated solely with the prevention of future incidents.

	Mil.	Thou.	Dol.
$	☐☐☐	☐☐☐	000

k. What other monetary losses and costs were incurred in 2005 due to these incidents? ESTIMATES are acceptable. INCLUDE actual losses such as the value of lost information. INCLUDE the estimated value of downtime, lost productivity, income from lost sales, abor or fees for legal or investigative work, etc.

	Mil.	Thou.	Dol.
$	☐☐☐	☐☐☐	000

13532

IV. OTHER TRENDS IN COMPUTER SECURITY

13. In 2005, did this company detect any computer security breaches that resulted from information obtained from a stolen laptop computer?

○ Yes → **How many incidents were detected?** ☐☐☐☐☐☐ Number

○ No

14. In 2005, was the overall number of computer security incidents detected by this company more, less or about the same compared to the number detected in 2004 regardless of whether damage or losses were sustained as a result? *Mark ● only one.*

○ More in 2005

○ Less in 2005

○ About the same

○ Don't know

15. In 2005, did this company have a separate insurance policy or rider to cover losses due specifically to computer security breaches?

○ Yes

○ No

○ Don't know

16. In 2005, what percentage of this company's business was transacted over the Internet, Intranet, Extranet, EDI, etc.?
ESTIMATES are acceptable.
INCLUDE any transaction completed over a computer-mediated network that involves the transfer of ownership or rights to use goods or services. For example, taking orders for merchandise or services, transferring information or rights, paying accounts, etc. ☐☐☐ %

V. COMPANY INFORMATION

17. In 2005, which of the following Internet services, if any, did this company provide to other companies or individuals as its PRIMARY line of business? *Mark ■ all that apply.*

☐ Internet Service Provider (ISP)

☐ Web Search Portal

☐ Other Internet service →Specify: _____

☐ None of the above

18 a. What were the total operating revenue, sales, and/or receipts for this company in 2005?
ESTIMATES are

	Bil.	Mil.	Thou.	Dol.
$	☐☐☐	☐☐☐	☐☐☐	000

b. What percentage of this total was derived from e-commerce?
ESTIMATES are acceptable.
INCLUDE any transaction completed over a computer-mediated network that involves the transfer of ownership or rights to use goods or services. For example, taking orders for merchandise or services, transferring information or rights, paying accounts, etc. ☐☐☐ %

19. What was the total number of employees on this company's payroll for the pay period which includes March 12, 2005?
ESTIMATES are acceptable. *Count EACH part-time employee as one.* ☐☐☐☐☐☐☐☐ Number
EXCLUDE contractors, vendors, leased and temporary employees.

20. Does the information reported in this survey cover calendar year 2005, fiscal year 2005 or some other time period?

○ Calendar year 2005

○ Fiscal year 2005 or some other time period →Specify period covered:

FROM: ☐☐ ☐☐☐☐ (Month Year) TO: ☐☐ ☐☐☐☐ (Month Year)

21. Does the information reported in this survey include this company or does it include this company and some or all of its subsidiaries?
For this survey, subsidiary means a company in which this company has more than 50% ownership, or in which this company has the power to direct or cause the direction of management and policies.

○ Information includes this company only - company has no subsidiaries, or responses exclude subsidiaries

○ Information includes this company and some or all of its subsidiaries - **How many subsidiaries were included?** ☐☐☐ Number

13532

(Tear off sheet - identifying information will be separated from survey responses upon receipt by RAND.)

CONTACT INFORMATION

Person to contact regarding this report:

Name

Title

Company Name

Phone ( ) - Ext.

Fax ( ) -

E-mail address

Please list subsidiaries included in this report:

REMARKS

(Please use this space or a separate sheet of paper for any explanations that may be essential in understanding your reported data.)

13532

U.S. DEPARTMENT OF JUSTICE
BUREAU OF JUSTICE STATISTICS
In partnership with the
U.S. DEPARTMENT OF HOMELAND SECURITY
NATIONAL CYBER SECURITY DIVISION

2005 NATIONAL COMPUTER SECURITY SURVEY INSTRUCTIONS

PURPOSE OF THE SURVEY

The purpose of this survey is to collect information about the nature and extent of computer security incidents experienced by businesses located in the U.S. The data you report will provide information on the impact of computer crime on businesses.

Specifically, data from the 2005 National Computer Security Survey will provide information on the frequency and types of crime involving computers, the monetary losses sustained as a result of computer crime, and the cost of computer security.

LEGAL AUTHORITY AND CONFIDENTIALITY

Your report is confidential by law (P.L. 107-347, Title V and 44 U.S.C. § 3501 note). It may be seen only by persons certified to uphold the confidentiality of this information and used only for statistical purposes from which no firm may be identified. The law also prohibits the sharing of your data with other agencies, exempts the information you provide from requests made under the Freedom of Information Act, and ensures that your responses are immune from legal process.

BURDEN HOUR ESTIMATE

Respondents are not required to respond to any information collection unless it displays a valid approval number from the Office of Management and Budget. Public reporting burden for this collection of information is estimated to vary from 45 minutes to 3 hours per response, with an average of 1½ hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Bureau of Justice Statistics, National Computer Security Survey, Washington, DC 20531; and to the Office of Management and Budget, OMB No. 1121-0301, Washington, DC 20503.

GENERAL INSTRUCTIONS

Survey Scope – This survey collects computer security data for companies, organizations and associations operating within the United States. **Information for business-related activities of religious organizations, nonprofit organizations and organizations that are government owned but privately operated should be included.**

Reporting Entity – Report computer security data for all **domestic operations** of your company, including all divisions and locations. A company is a business, service or membership organization consisting of one or more establishments under common ownership or control**. Do not report for subsidiary companies that your company may hold, as they may be surveyed separately.** For this survey, subsidiary means a company in which this company has more than 50% ownership, or in which this company has the power to direct or cause the direction of management and policies. *Use figures that include subsidiaries only if figures that exclude subsidiaries are not available.* For purposes of this survey, exclude data for Puerto Rico, the Virgin Islands and U.S. Territories. If you are unable to consolidate records for the entire company minus subsidiaries or have reporting questions, please call **1–800–734-5399.**

How to Report Dollar Figures – Dollar figures should be **rounded** to thousands of dollars.

For example, if the figure is $1,023,528.79, enter:

Mil.	Thou.	Dol.
$ 1	0 2 4	

If the figure is less than $500.00, enter:

Mil.	Thou.	Dol.
$	0	

Estimates are acceptable – The data requested on the National Computer Security Survey may not correspond to your company's records. If you cannot answer a question from your company records, please provide a carefully prepared estimate.

Reporting Period – Report data for calendar year 2005. If you cannot provide data on a calendar year basis, fiscal year 2005 data are acceptable. If this company was not in operation for the full year, report for the period of time it was in operation. Indicate in Question 20, Report Period, the exact dates the data represent if they are not for the calendar year.

Additional Forms – Photocopies of this form are acceptable. If you require additional forms, contact us at the toll-free number, e-mail address, or business address provided below.

Filing the Report Form – Return your completed form in the pre-addressed envelope. If you are not using the pre-addressed envelope, return it to the address provided at the bottom of this page or fax it to 1–877-814-6673.

RAND Corporation
Survey Research Group
1776 Main Street
P.O. Box 2138
Santa Monica, CA 90407-2138

Direct any **QUESTIONS** regarding this form to:

Toll-free Number: 1-800-734-5399
FAX Number: 1-877-814-6673
E-mail: ncss@rand.org

GLOSSARY OF TERMS

Adware – A software application that automatically displays advertisements, typically in the form of pop-up windows. Adware sometimes includes spyware.

Anti-spyware/adware software – A utility that looks for spyware and/or adware and alerts the user to any that are found.

Anti-virus software – A utility that looks for viruses and alerts the user to any that are found.

Biometrics – Methods of generating authentication information for a person by digitizing measurements of a physical characteristic, such as a fingerprint, a hand shape, a retinal pattern, a speech pattern (voice print), or handwriting.

Business continuity plan for computer systems – The procedure an organization uses to maintain essential functions during and after a disaster, such as a dual back-up system at a separate physical location. It seeks to ensure the uninterrupted provision of mission-critical functions. It often includes a disaster recovery plan.

Company laptops – Any laptop computer issued by this company, whether owned or leased.

Computer/network watch center – The location from which control is exercised over a communications network, usually either telephony or Internet, though sometimes also that of a public utility. It is sometimes also the location containing many or all of the primary servers and other equipment that runs an internet service provider. This center is also where the technicians that maintain the servers, develop new software, and troubleshoot outages are located.

Configuration management – The management of security features and assurances through control of changes made to hardware, software, firmware, documentation, test fixtures, and test documentation of an automated information system, throughout the development and operational life of a system. Includes Source Code Management or revision control. The control of changes—including the recording thereof—that are made to the hardware, software, firmware, and documentation throughout the system lifecycle.

Corporate policy on computer security – A defined set of practices and guidelines established by the organization to deal with issues involving computer security. Such practices and guidelines can encompass the responsibilities of both the organization and its employees. Employees have been made aware of this policy.

Digital certificates – An attachment to an electronic message used for security purposes. The most common use of a digital certificate is to verify that a user sending a message is who he or she claims to be, and to provide the receiver with the means to encode a reply.

Disaster recovery plan for computer systems – A procedure to restore an organization's mission-critical functions after, and to minimize the effects of, a major interruption of computer services. It includes procedures for reporting specific types of problems to designated personnel, repairing or replacing damaged systems, etc.

DMZ Host – A small network that acts as a "neutral zone" between a company's internal network and an external network such as the Internet. A DMZ host is usually inserted behind or between firewalls.

Electronic Data Interchange (EDI) – A proprietary electronic system used for exchanging business data over a computer network.

E-mail logs or filters – E-mail logs keep track of incoming/outgoing messages, including the sender and the recipient. Filters are an automated method of searching the content of e-mail for words, viruses, or misuse of computer resources.

Encryption – The translation of data into a format that requires a code to restore it to the original format. To read an encrypted file, you must have access to a secret key or password that allows you to decrypt it.

Equipment decommissioning – A procedure used for removing computer equipment from active use within an information system or network. This involves changing settings within the system to reflect their absence, and the removal of all sensitive information from the computer equipment, particularly from hard drives and other media.

External computer security controls – Hardware, software, and/or company policies and practices limiting the access of outsiders to the company's computer systems and networks.

Extranet – A network that uses Internet/Intranet technology to make information available to authorized outsiders. It allows businesses to securely share information with selected suppliers, partners, customers, or other businesses.

Firewall – Hardware and/or software designed to prevent unauthorized access to or from a private network, particularly networks with Internet or Intranet connectivity.

Formal computer security audit standards – An established or authoritative set of criteria used to review computer security systems.

Hacker – An unauthorized person who cracks a computer system or exceeds authorized access for malicious intent or for the thrill of the challenge.

Hard-wired telecommunication lines – Telecommunication lines that are copper or fiber-optic and stationary, as opposed to wireless.

Identification of company's critical assets – Determining the critical functions that the organization performs, and the assets (such as information and telecommunication systems) upon which those functions are vitally dependent. Those critical assets are ones for which special security and reliability measures should be focused.

Insurance covering computer security breaches – This type of insurance specifically covers losses due to computer break-in exposures, usually in a separate policy or rider. The coverage is typically called network security liability, e-commerce liability, Internet security liability, or hacker insurance.

Internal computer security controls – Hardware, software, and/or company policies and practices limiting the access of insiders—employees, contractors, vendors, etc.—to the company's computer systems or networks. These controls may vary by department and/or employee function.

Internet – Inter-connected networks linking millions of computers globally. Users can access information and applications from other computers and communicate with other users.

Intranet – An internal network similar to the Internet but surrounded by a firewall to prevent access from users outside the company, organization, or facility.

Intrusion detection system – An intrusion detection system examines all inbound and outbound network activity and identifies suspicious patterns that may signal a network or system attack from someone attempting to break into or compromise a system.

Intrusion/penetration testing of computer security – A method of evaluating the security of a computer system and identifying its vulnerabilities by attempting to circumvent or override system security through the simulation of an attack by a malicious actor.

Intrusion protection system – A suite of access control tools used to protect computers from exploitation. Intrusion protection systems may also act at the host level to deny potentially malicious activity.

Local area network (LAN) – A computer network that spans a small area such as a single building or group of buildings.

Malware – Malicious software or code developed to serve a harmful purpose. Specific types of malware include viruses, worms, Trojan horses, spyware, and adware.

Misuse of computers by employees (Internet, e-mail, etc.) – The improper use of company computer resources by employees, such as using the company's computer resources for personal gain, sending personal or improper e-mail, abusing Internet privileges, loading unlicensed software, etc.

Non-company laptop – Any laptop computer not issued by this company (e.g., belonging to a consultant, vendor, contractor, etc.).

One-time password generators (smart cards, tokens, keys) – A "one-time password generator" is an authentication device such as a one-time token which randomly changes all or part of the user's password, typically every minute, so that the same password is never used more than once. This technique counters the threat of a replay attack that uses passwords captured by spyware, wiretapping, or other means of hacking.

Passwords that must be changed periodically – A simple authentication technique in which each password is used repeatedly for a specific period of time to verify an identity.

Periodic computer security audits – Reviews conducted periodically by the company's security office. For example, the company's strike team might simulate computer security situations and then evaluate how the company performed.

Phishing – The creation and use of fraudulent but legitimate-looking e-mails and web sites to obtain users' personal and financial account information for criminal purposes.

Physical/environmental security (e.g., limited physical access, sprinklers) – Security measures focused on limiting physical access to critical organization assets, and protection of those assets from physical malicious attacks (e.g., explosions) or natural disasters (earthquakes, fire, flood).

Pinging – A basic test of whether a particular host is operating properly and is reachable on the network from the testing host by sending a special packet of information and awaiting its response. Malicious use includes flooding the Internet with ping requests attempting to locate new hosts to infect, causing problems to routers across the Internet.

Piracy – see Unlicensed use or copying.

Process control network (PCN) – A network with an automated control of a process, such as a manufacturing process or assembly line. It is used extensively in industrial operations, such as oil refining, chemical processing, and electrical generation. It uses analog devices to monitor real-world signals and digital computers to do the analysis and controlling. It makes extensive use of analog/digital, digital/analog conversion.

Publicly accessible website WITH e-commerce capabilities – E-commerce capabilities refer to the ability of this company's customers or suppliers to effect transactions via computer networks. Such transactions commit the company and the customer/supplier to an exchange, though they do not necessarily include making payment associated with the commitment. For example, if a customer orders products via a website with payment made by check at a later date, this is an e-commerce transaction.

Regular review of system administrative logs – Reviewing system administrative logs on a regular basis to detect suspicious activity beyond normal daily activity.

Remote dial-in access – Refers to using devices and other resources that are not connected directly to a workstation to connect to another computer device. Do not include network access through the Internet.

Scanning – A method of searching for open ports by sending packets or requests for information.

Server – A computer or device on a network that manages network resources. For example, a file server is a computer and storage device dedicated to storing files. A print server is a computer that manages one or more printers. A network server is a computer that manages network traffic.

Sniffing – Packet sniffing is a form of wire-tap applied to computer networks instead of phone networks. Traffic on a network segment passes by all hosts attached to that segment. Ethernet cards have a filter that prevents the host machine from seeing traffic addressed to other stations. Sniffing programs turn off the filter, and thus see everyone's traffic.

Spoofing – The creation of TCP/IP packets using someone else's IP address. A "spoofed" IP address is therefore misleading regarding the true source of an Internet message packet.

Spyware – Software that surreptitiously monitors the user and transmits the information to a third party. Some spyware can intercept or take partial control of a computer's operation. Spyware differs from viruses and worms in that it does not usually self-replicate.

Stand-alone PCs (not on LAN) – Computers that are not connected to company networks, such as a stand-alone workstation. For the purposes of this survey, a stand-alone computer may have Internet access.

System administrative logs – Logs which document details of access to computer systems, such as who logged in, which parts of the system were accessed, and when the user logged in and out.

Training employees in computer security practices – Training session(s) designed to educate employees on issues dealing with computer security and the employee's role in following the organization's computer security practices.

Trojan horse – A program that overtly does one thing while covertly doing another.

Unlicensed use or copying (piracy) of digital products developed for resale – The unauthorized copying or use of digital products — such as software, music, or motion pictures — which the company developed or for which it holds the copyright. Report unauthorized copying or use of other software by employees under "Misuse of computers by employees (Internet, e-mail, etc.)."

Virtual private network (VPN) – A network that is constructed by using public wires to connect nodes. For example, systems that allow you to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network.

Virus – A hidden fragment of computer code which propagates by inserting itself into or modifying other programs.

Vulnerability/risk assessment – Assessment of threats to, impacts on, and vulnerabilities of information and information-processing facilities and the likelihood of their occurrence.

Wide area network (WAN) – A computer network that spans a large geographical area. Usually, a WAN consists of two or more LANs.

Wireless networks (e.g., 802.11) – A type of LAN that uses high-frequency radio waves or lasers rather than wires to communicate between nodes. 802.11 refers to a family of specifications for an over-the-air interface between a wireless client and a base station or between two wireless clients.

Wireless access to e-mail, Internet and/or this company's other networks – Wireless access refers to the use of a device or system that will enable access to a network to which it is not physically connected. For example, access via a cellular or digital phone, some personal digital assistants (PDAs), some laptop computers, thin client, broadband, etc.

Worm – A self-replicating computer program, similar to a computer virus. A virus attaches itself to, and becomes part of, another executable program; however, a worm is self-contained and does not need to be part of another program to propagate itself. They are often designed to exploit the file transmission capabilities found on many computers.