



JUSTICE, INFRASTRUCTURE, AND ENVIRONMENT

Estimating the Global Cost of Cyber Risk

Methodology and Examples

Paul Dreyer, Therese Jones, Kelly Klima, Jenny Oberholtzer, Aaron Strong,
Jonathan William Welburn, Zev Winkelman

Sponsored by the William and Flora Hewlett Foundation
and the CyberCube unit of the Symantec Corporation

For more information on this publication, visit www.rand.org/t/RR2299

Published by the RAND Corporation, Santa Monica, Calif.

© Copyright 2018 RAND Corporation

RAND® is a registered trademark.

Limited Print and Electronic Distribution Rights

This document and trademark(s) contained herein are protected by law. This representation of RAND intellectual property is provided for noncommercial use only. Unauthorized posting of this publication online is prohibited. Permission is given to duplicate this document for personal use only, as long as it is unaltered and complete. Permission is required from RAND to reproduce, or reuse in another form, any of its research documents for commercial use. For information on reprint and linking permissions, please visit www.rand.org/pubs/permissions.

The RAND Corporation is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest.

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

Support RAND

Make a tax-deductible charitable contribution at
www.rand.org/giving/contribute

www.rand.org

Preface

Cyber incidents have been increasing in frequency and cost in recent years, with some resulting in hundreds of millions of dollars in losses. There is marked variability from study to study in the estimated direct and systemic costs of cyber incidents, which is further complicated by the considerable variation in cyber risk across countries and industry sectors. In many cases, comparing research studies is complicated by a lack of transparency in methodologies, assumptions, and data sets used. The goal of this research was to produce a transparent methodology for estimating present and future global costs of cyber risk, acknowledging the considerable uncertainty in the frequencies and costs of cyber incidents. A companion Excel tool implements the methodology described in this document.¹ This research was sponsored by the William and Flora Hewlett Foundation and the CyberCube unit of the Symantec Corporation and will be of interest to researchers and policymakers involved with cyber risk assessment and mitigation.

RAND Science, Technology, and Policy

The research reported here was conducted in the RAND Science, Technology, and Policy program, which focuses primarily on the role of scientific development and technological innovation in human behavior, global and regional decisionmaking as it relates to science and technology, and the concurrent effects that science and technology have on policy analysis and policy choices. The program covers such topics as space exploration, information and telecommunication technologies, and nano- and biotechnologies. Program research is supported by government agencies, foundations, and the private sector.

RAND Justice, Infrastructure, and Environment (JIE) conducts research and analysis in civil and criminal justice, infrastructure development and financing, environmental policy, transportation planning and technology, immigration and border protection, public and occupational safety, energy policy, science and innovation policy, space, telecommunications, and trends and implications of artificial intelligence and other computational technologies.

Questions or comments about this report should be sent to the project leader, Paul Dreyer (Paul_Dreyer@rand.org). For more information about RAND Science, Technology, and Policy, see www.rand.org/jie/stp or contact the director at stp@rand.org.

¹ Dreyer, 2018.

Contents

Preface.....	iii
Figures.....	vi
Tables.....	vii
Summary.....	viii
Acknowledgments.....	x
Abbreviations.....	xi
Symbols.....	xii
 Chapter 1: Introduction.....	 1
Summary of Existing Global Cyber Cost Estimate Research and Results.....	1
Report Objective and Outline.....	3
Chapter 2: Modeling the Costs of Cyber Risk.....	4
Model Structure.....	4
Direct Costs at the Sector and Country Levels.....	5
From Direct to Systemic Costs.....	6
Projecting Future Costs.....	9
Chapter 3: Model Parameters.....	10
Sets.....	10
Country (C).....	10
Industry Sectors (I).....	10
Financial Exposures (E).....	11
Perils (P).....	12
Mapping Notable Cyber Incidents to Sets.....	13
Relations Between Sets.....	15
Country-Specific Sector Weights (w_{ci}).....	15
Sector-Exposure Relationship (Y_{cie}).....	16
Exposure-Peril Relationship (X_{ciep}).....	20
Alternative Method for Directly Estimating Potential Economic Damage.....	21
Chapter 4: Case Studies.....	24
Global Cost of Cyber Crime.....	26
Cost of Cyber Crime in the Netherlands (1.27 Percent of GDP).....	28
Sample Case Study: Lloyd's Business Blackout.....	32
Sensitivity to the Choice of Probability Distribution Functions.....	33
Chapter 5: Conclusion and Next Steps.....	35
Appendix A: Estimating the Global Cost of Cyber Risk Calculator User Manual.....	37
Appendix B: Review of Model Assumptions.....	41
Appendix C: Module Y2 Sector-Exposure Relationship.....	43

Appendix D: Advisen Data.....	45
Appendix E: Characterizing Attackers and Perils	46
Appendix F: Potential Expert Elicitation Format	47
References.....	49

Figures

Figure 4.1. Comparison of Models 1, 2, and 3	25
Figure 4.2. Cost of Global Cyber Crime, Model 1: Breakout of Damages by Sector	26
Figure 4.3. Cost of Global Cyber Crime, Model 2: Breakout of Damages by Sector	27
Figure 4.4. Cost of Global Cyber Crime, Model 3: Breakout of Damages by Sector	28
Figure 4.5. Cost of Cyber Crime in the Netherlands, Model 1: Distribution of Total GDP Costs.....	29
Figure 4.6. Cost of Cyber Crime in the Netherlands, Model 1: Breakout of Damages by Sector	29
Figure 4.7. Cost of Cyber Crime in the Netherlands, Model 2: Distribution of Total GDP Costs.....	30
Figure 4.8. Cost of Cyber Crime in the Netherlands, Model 2: Breakout of Damages by Sector	30
Figure 4.9. Cost of Cyber Crime in the Netherlands, Model 3: Distribution of Total GDP Costs.....	31
Figure 4.10. Cost of Cyber Crime in the Netherlands, Model 3: Breakout of Damages by Sector	31
Figure 4.11. Cost of Cyber Crime in the Netherlands, Model 3: Breakout of Damages by Sector	34
Figure D.1. Exceedance Probability of Costs for Each Event Type.....	45

Tables

Table S.1. Summary of Case Study Results for Different Models	ix
Table 3.1. Advisen Data Set Case Types Mapped to Event Types.....	12
Table 3.2. Perils (p) and Exposures (e) of Notable Cyber Incidents, by Sector (i) and Country (c)	14
Table 3.3. Module Y1: Dutch Sector-Exposure Relationship (Y_{cie}) as Given in Literature, Unitless	16
Table 3.4. Results of Sector-Exposure Regression, Unitless.....	19
Table 3.5. Module Y2: SEC Sector-Exposure Relationship (Y_{cie}), Unitless	19
Table 3.6. Mapping Deloitte's Threats to Our Model Perils	20
Table 3.7. Module X1: Dutch Peril-Exposure Relationship (X_{cep}), Unitless	21
Table 3.8. 25th-, 50th-, 75th-, and 95th-Percentile Bootstrapped Values of Direct Costs in the United States for Each Sector as a Percentage of Revenue	22
Table 3.9. Sector Output Weights for the United States ($w_{USA,i}$)	22
Table 3.10. Determination of U.S. GDP at Risk Using Bootstrapped Values of Direct Costs in the United States for Each Sector as a Percentage of Revenue	23
Table 3.11. Module 3: Value at Risk Exposure-Peril Relationship (X_{cep}), Unitless	23
Table 3.12. Module 3: Value at Risk Sector-Exposure Relationship (Y_{cie}), Unitless	23
Table 4.1. Summary of Case Study Results for Different Models	25
Table 4.2. Model 3: Capital Assets Sector Exposure Best Fits for Different Distributions	34
Table A.1. Probability Distributions Allowed in Calculator	39
Table C.1. Results of Sector-Exposure Regressions: R&D	43
Table C.2. Results of Sector-Exposure Regressions: Net Income.....	43
Table C.3. Results of Sector-Exposure Regressions: Total Assets.....	43
Table E.1. Attacker and Threat Characterizations	46
Table F.1. Pain-Level Elicitation Worksheet.....	47
Table F.2. Sector Variation Elicitation Worksheet.....	48

Summary

Cyber incidents have been increasing in frequency and cost in recent years, with some resulting in hundreds of millions of dollars in losses. There is marked variability from study to study in the estimated direct and systemic costs of cyber incidents, which is further complicated by the considerable variation in cyber risk across countries and industry sectors. In many cases, comparing research studies is complicated by a lack of transparency in methodologies, assumptions, and data sets used. For example, some previous research has focused on the likelihood or probability of perils; unfortunately, due to a lack of publicly available data, it is difficult to convert these data to a transparent tool.

The goal of this research was to produce a transparent and adaptable methodology for estimating present and future global costs of cyber risk that acknowledges the considerable uncertainty in the frequencies and costs of cyber incidents. This methodology (1) identifies the value at risk by country and industry sector; (2) computes **direct costs** by considering multiple financial exposures for each industry sector and the fraction of each exposure that is potentially at risk to cyber incidents; and (3) computes the **systemic costs** (also known as *upstream costs* or *knock-on costs*) of cyber risk between industry sectors using Organisation for Economic Co-operation and Development input, output, and value-added data across sectors in more than 60 countries. To incorporate uncertainty into the model, we allowed many of the parameters to be defined by point estimates or probability distributions. In our model, we include uniform, triangular, trapezoidal, generalized beta, and Delphi distributions (the latter involving a set of values or distributions, often in response to elicitation from multiple subject-matter experts, that are equally likely to be chosen). Outputs are either average values or cumulative distributions of these costs across countries and sectors.

This report has a companion Excel-based modeling and simulation platform that allows users to alter assumptions and investigate a wide variety of research questions.² We highlight this functionality by using both a literature review and gathered data to create multiple sample sets of parameters. We then ran a set of case studies to demonstrate the model's functionality and to compare the results against those in the existing literature (Table S.1). We found that resulting values are highly sensitive to input parameters; for instance, using three reasonable sets of parameters from existing research and our own data analysis, we found that cyber crime has a direct gross domestic product (GDP) cost of \$275 billion to \$6.6 trillion globally and total GDP costs (direct plus systemic) of \$799 billion to \$22.5 trillion (1.1 to 32.4 percent of GDP). The purpose of the tool we have developed is to make transparent the underlying assumptions that go into these calculations of the cost of cyber risk.

² Dreyer, 2018.

These sample sets are meant to illustrate potential uncertainties and related studies; users will likely want to update model assumptions to investigate their research question of choice. Sample questions that could be addressed with this model include the following: What is the global cost of cyber crime? How much direct damage could a cyber-induced blackout incur? Do Bayesian priors from an expert elicitation reduce model sensitivity to inputs? How will cyber controls affect costs? The current model estimates upstream systemic costs; future versions will attempt to estimate downstream costs as well.

Table S.1. Summary of Case-Study Results for Different Models

Case Study	Literature	Model 1: Dutch Peril and Exposure Estimates	Model 2: Dutch Peril and SEC Estimates	Model 3: VaR Direct Estimates	Model Implementation of Lloyd's Study
1. Global cost of cyber crime	See Chapter 1	Direct: \$275 billion Total: \$799 billion (1.1% of global GDP)	Direct: \$3.2 trillion Total: \$10.1 trillion (14.5% of global GDP)	Direct: \$6.6 trillion Total: \$22.5 trillion (32.4% of global GDP)	N/A
2. Cost of cyber crime in the Netherlands	1.5% of Dutch GDP	Direct: \$3.4 billion Total: \$9.9 billion (1.26% of Dutch GDP)	Direct: \$35.9 billion Total: \$113.8 billion (14.6% of Dutch GDP)	Direct: \$84.1 billion Total: \$291.3 billion (37.3% of Dutch GDP)	N/A
3. Lloyd's business blackout	\$243 billion to \$1.024 trillion, depending on scenario	N/A	N/A	N/A	Direct: \$184 billion Total: \$515 billion

NOTES: SEC = U.S. Securities and Exchange Commission; VaR = value at risk.

Acknowledgments

The authors would like to thank our project sponsors, the Hewlett Foundation and the CyberCube unit of the Symantec Corporation, for their support of this research. Special thanks to Eli Sugarman and Hauwa Otori from the Hewlett Foundation and Michael Varshavski, Morgan Hervé-Mignucci, and Pascal Millaire from the CyberCube unit of the Symantec Corporation for providing their insight and guidance. Additionally, thanks to the project steering committee: Michael Chertoff (the Chertoff Group), Tim Francis (the Travelers Companies), Alice Gugelev (HighPoint Associates), Melissa Hathaway (Potomac Institute), Erin Kenneally (U.S. Department of Homeland Security), Donald Mango (Columbia University), Bruce Schneier (IBM Resilient), Richard Tischer (Zurich Insurance Group), George Triantis (Stanford University), and Steve Weber (University of California, Berkeley). Thanks to Sasha Romanosky, Lily Ablon, and Sarah Nowak from RAND for their insights and assistance. And finally, thanks to the Chertoff Group, particularly Michael Chertoff, Katy Montgomery, and Adam Isles, for reviewing our document and Excel tool.

Abbreviations

CGE	computable general equilibrium
DDoS	distributed denial of service
GDP	gross domestic product
IP	intellectual property
NIST	National Institute of Standards and Technology
OECD	Organisation for Economic Co-operation and Development
PII	personally identifiable information
R&D	research and development
RDM	Robust Decision Making
SAM	social accounting matrix
SEC	U.S. Securities and Exchange Commission
STAN	Structural Analysis Database
USD2016	2016 U.S. dollars
VaR	value at risk

Symbols

Variable	Units	Description
β_n		coefficient in regression equation
A_c		input-output matrix that defines how production takes place
$c \in C$	N/A	c is a particular country within the set (C) of countries
d_{co}	USD2016	direct output losses as a function of country
d_{cg}	% of GDP	direct GDP losses as a function of country
d_{cio}	USD2016	direct output losses as a function of country and industry sector
d_{cig}	USD2016	direct GDP losses as a function of country and industry sector
$e \in E$	N/A	e is the financial exposure within the set (E) of financial exposures that could possibly be harmed, independent of hazard type
F_c		vector of final demands
G_c	USD2016	GDP of country c
$i \in I$	N/A	i is a particular industry sector within the set (I) of industry sectors
I_n		identity matrix
n	unitless	index (e.g., within identity matrix)
O_{ci}	USD2016	sector output for country c and industry sector i
$p \in P$	N/A	p is the peril with the set (P) of perils where a cyber attack's actions on objectives may result in costs realized by the defender
s_{co}	USD2016	systemic output losses as a function of country
s_{cg}	USD2016	systemic GDP losses as a function of country
s_{cio}	USD2016	systemic output losses as a function of country and industry sector
s_{cig}	USD2016	systemic sector GDP losses as a function of country and industry sector
X_{ciep}	unitless	the fraction of the exposure at risk in country (c), industry sector (i), and exposure type (e) that will be successfully destroyed, stolen, or otherwise lost due to a particular peril (p)
Y_{cie}	unitless	the fraction of the quantity $w_{ci} * G_c$ that is equivalent to the amount of money at risk from each exposure type (e), regardless of whether they can be harmed by a cyber attack
z_{cij}		entry in the i^{th} row and j^{th} column of $(I_n - A_c)^{-1}$

Chapter 1: Introduction

In recent years, cyber incidents have increased in frequency and cost, with some resulting in hundreds of millions of dollars in losses. There is marked variability from study to study in the estimated direct and systemic costs of cyber incidents, which is further complicated by the considerable variation in cyber risk across countries and industry sectors. In many cases, comparing research studies is complicated by a lack of transparency in methodologies, assumptions, and data sets used.

Summary of Existing Global Cyber Cost Estimate Research and Results

We explored cyber cost data from more than 550 sources, including journal articles, reports, and websites.³ Some of these sources focused on catastrophic loss scenarios in different economic sectors, and some focused on the global costs of cyber crime. In general, authors agreed that the annual cost to the global economy is highly uncertain but is likely on the order of hundreds of billions of dollars. For example, McAfee and the Center for Strategic and International Studies⁴ and Lloyd's⁵ estimated the annual cost at \$375 to \$575 billion and \$400 billion, respectively. Juniper Research estimated that breaches would cost \$2.1 trillion in 2019 (four times the 2015 value).⁶

To better understand reporting methods, we used 15 reports from reputable sources⁷ to collect approximately 590 distinct cost data points on chronic (not catastrophic) losses.⁸ Many of these data were aggregated by sector, company size, or country (possibly to protect the privacy of the reporting entities), making it difficult to conduct regressions with any certainty. Of the data points collected, we found that 60 percent of the costs were total costs, 10 percent were aggregated immediate response costs, 9 percent were aggregated direct costs, 8 percent were reputational losses, 8 percent were aggregated costs after the immediate response costs, and the remainder were other costs. While this finding is a function of the reports reviewed, it suggests that the state of the art of data reporting leans toward aggregation, and, thus, it may be difficult to use regression to characterize specific dependencies.

³ List available upon request.

⁴ McAfee and the Center for Strategic and International Studies, 2014.

⁵ Gandel, 2015; we note that this is a *Fortune* article referencing a Lloyd's chief executive officer, but we could not find the original Lloyd's report.

⁶ Juniper Research, 2015.

⁷ Advisen, 2010; Ponemon Institute, 2012; Gagnaire et al., 2012; Ponemon Institute, 2013a; Ponemon Institute, 2013b; Ponemon Institute, 2014; Association for Financial Professionals, 2015; McAfee and the Center for Strategic and International Studies, 2014; Kaspersky Lab, 2015; Ponemon Institute, 2015; Federal Bureau of Investigation, 2016; Hiscox, 2017; NetDiligence, 2016; Ponemon Institute, 2016; Ponemon Institute, 2017.

⁸ Collected data available upon request.

Next, we examined data collection and modeling methods. One common method is to **survey companies and anonymize the voluntarily reported data**. For instance, Ponemon Institute's 2017 Cost of Data Breach study collected survey data on the scope and magnitude of data breaches in 419 companies across 11 countries, finding that the average data breach cost was \$3.62 million, or \$141 per lost or stolen record.⁹ In that year, the companies faced 312,376 breaches, at a total cost of \$1.01 trillion. Per capita costs varied widely by country, with highest costs in the United States and Canada (\$225 and \$190 per capita) and the lowest in Brazil and India (\$79 and \$64 per capita). Costs were also far higher for health care (\$380) and financial services (\$249) than for media (\$119), research (\$101), and the public sector (\$71). Another common method is to **survey employees and anonymize the voluntarily reported data**. Hiscox (2017) surveyed 3,000 information technology specialists across the United States, United Kingdom, and Germany and found that the average cost of a company's largest cyber incident over the previous year varied from €22,000 to \$102,000, depending on the country and company size.¹⁰ Similarly, Kaspersky Lab (2015) examined 5,500 businesses in 2,200 countries and found that enterprise businesses (with more than 1,500 employees) lose \$500,000 on average from security breaches, and small and medium businesses lose \$38,000 on average.¹¹ A third method is to **model the cost of different attack scenarios on various sectors**. Lloyd's (2017) examines the risk of cloud service provider interruption and cyber mass vulnerabilities by considering hypothetical scenarios of widely adopted technologies in industry, nontechnical factors, cybersecurity risk factors, and the exposure accumulation path.¹² They found extreme-value losses for cloud service provider interruption of \$4.6 billion and \$9.68 billion and for cyber mass vulnerability of \$53.05 billion and \$28.72 billion. A second modeling method is Gagnaire et al.'s 2012 estimation that the outage of 13 cloud services from 2007 to 2012 cost \$71.7 billion, based on "hourly costs accepted in the industry."¹³ Perhaps the least common method is to **report collected data on actual attacks**. For instance, Symantec's study on ransomware and business found that reported worldwide ransom demand averaged around \$679 per incident.¹⁴ In general, due to both privacy concerns and opaqueness of models, assumptions, and data sources, reporting appears to lean toward anonymization, and, thus, it is difficult to provide transparency in a model.

The wide variation in costs shown in the literature review, with a minimal amount of explanations regarding the derivation of the results, suggests a clear need for a reputable, transparent model that many organizations or individuals could build on to create comparable analyses. In addition, we find that almost all documents focus on direct or indirect costs to a company; there was much less discussion on the macroeconomic impacts experienced by other sectors because of the focus on direct damages by each sector.

⁹ Ponemon Institute, 2017.

¹⁰ Hiscox, 2017.

¹¹ Kaspersky Lab, 2015.

¹² Lloyd's, 2017.

¹³ Gagnaire et al., 2012.

¹⁴ Symantec, 2016.

Report Objective and Outline

The goal of this research was to produce a transparent and adaptable methodology for estimating present and future global costs of cyber risk that acknowledges the considerable uncertainty in the frequencies and costs of cyber incidents. This methodology (1) identifies the value at risk by country and industry sector; (2) computes **direct costs** by considering multiple financial exposures for each industry sector and the fraction of each exposure that is potentially at risk to cyber incidents; and (3) computes the **systemic costs** (also known as *upstream costs* or *knock-on costs*) of cyber risk between industry sectors using Organisation for Economic Co-operation and Development (OECD) input, output, and value-added data across sectors in more than 60 countries. To incorporate this uncertainty into the model, we allowed many of the parameters to be defined by point estimates or probability distributions. In our model, we include uniform, triangular, trapezoidal, generalized beta, and Delphi distributions (the latter involves a set of values or distributions, often in response to elicitation from multiple subject-matter experts, that are equally likely to be chosen). Outputs are either average values or cumulative distributions of these costs across countries and sectors. This report has a companion Excel-based modeling and simulation platform that allows users to alter assumptions and investigate a wide variety of research questions.¹⁵

Chapter 2 describes the model structure to estimate the direct and systemic costs of cyber incidents now and in the future. Chapter 3 describes the multiple methods we used to populate sample sets of parameters in the model. Chapter 4 gives a series of case studies that we use to show the model's functionality and to compare against existing results in the literature. Appendix A is the user manual for the companion tool, *Estimating the Global Cost of Cyber Risk Calculator*.¹⁶ Appendix B provides further detail on one of the module calculations. Appendix C discusses some of our model assumptions. Appendix D describes the Advisen data set. Appendix E describes potential cyber attackers and threats in more detail. Appendix F describes a potential expert elicitation form to estimate industry sector exposures to cyber risks.

¹⁵ Dreyer, 2018.

¹⁶ Dreyer, 2018.

Chapter 2: Modeling the Costs of Cyber Risk

Our goal was to produce a model to estimate the costs of cyber risk that was transparent and straightforward in its implementation but also captured the uncertainty in estimating the frequency and cost of cyber incidents. This chapter describes our model structure for estimating the global costs of cyber risk. This cost estimator is implemented in our Excel tool, and Appendix A contains a user manual for the Excel tool.

Model Structure

We developed a model to describe the impact that different cyber incidents have on the value-added gross domestic product (GDP) of industry sectors in a country. Model assumptions and consequent limitations are listed in Appendix B. To construct this model, we first defined the following four sets:

Countries: $c \in C$
Industry sectors: $i \in I$
Economic exposures: $e \in E$
Perils: $p \in P$

That is, we constructed a model with a set of countries C , industry sectors I , economic exposures E , and perils P . Thus, each country c is in the set of countries C , each industry sector i is in the set of industry sectors I , each financial exposure e is in the set of economic exposures E , and each peril p is in the set of perils P where a cyber attack's actions on objectives may result in costs realized by the defender. Sets are descriptors and thus are unitless.

Each set is defined to be independent of another but may not be mutually exclusive or collectively exhaustive. The set of countries C , for example, is a subset of total countries in the world, and its size depends on data availability. The set of industry sectors I is defined to be mutually exclusive and collectively exhaustive. While the sets of financial exposures E and perils P are intended to be both mutually exclusive and collectively exhaustive, the changing nature of cyber attacks may expand this set beyond the definitions currently within this model. We also assumed additive separability of direct costs, such that in calculating direct costs, subsets within each set do not affect each other but do interact through the broader systemic cost calculations.

In our analysis, we relate incident cost to GDP loss in specific industry sectors. This approach both accounts for rebound effects between companies (where a loss by one company could result in a gain at another) and reduces the need to aggregate over a variety of widely uncertain cost types. Specifically, we divide costs into (1) output losses experienced by each sector i in each country c (**direct** [d_{ci}] units of 2016 U.S. dollars [USD2016]) and (2) the macroeconomic impacts to output experienced by other sectors because of the direct damages by each sector i in each country c (**systemic** [s_{ci}] units of USD2016). In this definition, direct costs

include costs that are directly paid by a sector before, during, and after an event, including damages in the form of attests, fines, extortion and investigative costs, and business interruptions that occur in the sector that was attacked, as well as litigation costs that may be incurred by third parties but are compensated by the firm that was attacked.

The main output of the model is twofold: the aggregate annual loss for each country directly due to cyber incidents, broken down by industry sector, as well as the systemic costs in each sector due to upstream disruptions caused by these incidents. A model run either produces the expected value of the costs given the underlying distributions of the input data or does a large number of draws on the underlying distributions to estimate the distribution function of the costs.

Direct Costs at the Sector and Country Levels

We calculated direct costs to output and GDP for each sector i in country c by relating the sets $(c, i, e, \text{ and } p)$ to G_c , the GDP of country c .

First, we define w_{ci} as sector i 's share of GDP in country c . Thus, $w_{ci} * G_c$ is the value added (contribution to GDP) of sector i in country c . Also, we define O_{ci} as the sector output of sector i in country c . Next, we define the unitless value Y_{cie} to be the fraction of industry sector output that is equivalent to the amount of money at risk from each exposure type (e), regardless of whether they can be harmed by a cyber attack. Finally, we define the unitless value X_{ciep} to be the fraction of the exposure at risk in country (c), industry sector (i), and exposure type (e) that will be successfully destroyed, stolen, or otherwise lost due to a particular peril (p).

Consequently, the product of Y_{cie} and X_{ciep} calculates the fractional impact of each cyber peril (p) on the output and/or value added of each sector i associated with each exposure e . Therefore, we can determine the direct cost to sector output in each sector i in country c by summing over the product $Y_{cie}X_{ciep}$ for all perils p and exposures e , which, multiplied by the output of sector i in country c (O_{ci}), gives the total sector direct costs to output as follows:

$$d_{cio} = O_{ci} \sum_{e \in E} \sum_{p \in P} Y_{cie} X_{ciep} \quad \forall i \in I, c \in C$$

Assuming changes in sector output scale to changes in sector GDP, one can similarly determine the direct costs to sector GDP, letting d_{cig} denote the loss to sector GDP:

$$d_{cig} = w_{ci} G_c \sum_{e \in E} \sum_{p \in P} Y_{cie} X_{ciep} = \frac{w_{ci} G_c}{O_{ci}} d_{cio} \quad \forall i \in I, c \in C$$

Furthermore, aggregating sector-level direct costs (d_{ci}) allows us to determine the total direct costs to output and GDP from cyber incidents for each country c as follows:

$$d_{co} = \sum_{i \in I} d_{cio} \quad \text{and} \quad d_{cg} = \sum_{i \in I} d_{cig} \quad \forall c \in C$$

Note that due to the complexity of dimensions and uncertainty in cyber attack scenarios, one might wish to examine how different model assumptions affect the well-understood quantity of $w_{ci} * G_c$, the GDP of country c that is in sector i . The resulting estimation will depend largely on the inputs of perils, exposures, sectors, and their relationships. Although identifying sectors and exposures is straightforward, estimating the impact of perils on exposures is a considerable challenge. While the next chapter discusses approaches for determining these relationships, considerable uncertainties will remain. Thus, the model is constructed to lay bare the uncertainties around these inputs by allowing users to alter input relationships and view the resulting changes in costs.

From Direct to Systemic Costs

In most previous analyses of the costs of cybersecurity,¹⁷ the approach ends by estimating the direct costs to an industry or sector. Our approach builds on the macroeconomic impact analysis to take the industry-level impacts and translate them into broader *systemic* economic impacts using an input-output model. When a disruption takes place within a firm, the costs are not necessarily contained within the firm, and there are broader supply-chain impacts that could be realized. Our approach allows for the inclusion of upstream impacts within the supply chain but not downstream. That is, the approach incorporates input suppliers to a sector that suffers an attack but does not incorporate the effects on sectors that use the output from the sector that has been attacked. Our analysis is done at the sectoral level rather than at the firm level because the sectoral-level networks are readily available across a wide variety of countries and we are estimating annual averages rather than the impact of specific attacks. If firm-level networks were available, the approach could be implemented at the firm level to better understand the impacts of cyber attacks on specific firms. Additionally, this would allow for the expansion of the impact to include the impact not only on input suppliers but also on output to customers.

There are generally two methods that have been employed to estimate macroeconomic impacts: input-output models and calibrated computable general equilibrium (CGE) models. There are advantages and disadvantages to both methods. The idea behind both approaches is to trace, through the supply and demand, responses following disruptions. When one industry faces a disruption, the input suppliers to that industry face a disruption as well. Further, because labor is a primary input to production, wages are lost from these disruptions, causing further shifts in demand for all products, as households have less money to spend on final products. The two methods differ on substitution between inputs to production. In the input-output approach, there is no substitution, and the production function acts like a recipe such that to double production, all inputs must double. With the CGE models, greater substitution is possible, and industry and household demand for products is a function of prices. As products become more expensive, substitutes are used in the production process or by households in terms of final demands.

The starting point for both approaches is the social accounting matrix (SAM). The SAM for an economy describes how all goods and services are produced, who owns the means of

¹⁷ Lloyd's, 2017; Deloitte, 2016.

production, and the set of final demands. This formulation of an economy allows for a full description of an economy at a specific point in time. In the United States, the Bureau of Economic Analysis produces these SAMs. OECD has developed SAMs for a variety of different countries.¹⁸

The input-output model assumes that the production functions are linear and come directly from the SAM. The input-output model is used to derive the economic multipliers that are commonly used in estimating economic impacts. The biggest advantage of the input-output model is its computational tractability arising from the linearity assumption regarding production functions.¹⁹ Because the supply chain is embedded within the SAM, it is simply a matter of matrix manipulation to obtain the economic impacts on other sectors as well as the economy as a whole. These advantages do come at a cost. In particular, for large disruptions, the lack of substitution within the production functions will tend to overestimate the impacts of a disruption. In addition, there are no prices included in the model, and production functions are based on values rather than quantities. Because input-output models are meant to consider small-scale changes relative to the economy, this should not be a particularly important problem.

As an alternative to input-output models, CGE models have been developed to allow for greater flexibility in the substitution patterns of production. To accomplish this, a larger number of parameters must be defined, and, in many instances, those parameters have not been estimated for every sector, so some “best guesses” are needed to calibrate CGE models. Additionally, because the CGE has prices, a larger number of impacts must be estimated. This leads to much greater computation complexity than can be accomplished in spreadsheet-type programs. CGEs seem more like black boxes for people not used to using them.

Input-output models are grounded in understanding the relationships within an economy. To satisfy a set of final demand for all products, the economy must produce more than the final demand because some of the products are used as inputs to the production of other products. For each country c , let V_c be a vector of production levels, F_c the vector of final demands, and A_c the input-output matrix that defines how production takes place. Then we know that the production levels must satisfy the intermediate demand as inputs to production as well as final demand by consumers. Thus, for the economy to be in equilibrium, defined by supply equaling demand, it must satisfy $V_c = A_c V_c + F_c$. We can transform this problem into $I_n V_c - A_c V_c = F_c$, or $V_c = (I_n - A_c)^{-1} F_c$, where I_n is the $n \times n$ identity matrix. $(I_n - A_c)^{-1}$ is called the *Leontief inverse matrix* and describes how output changes with changes in demand. Each entry in the Leontief inverse matrix describes how a change in the output of one industry impacts the output in another. The column sums of the Leontief inverse matrix are the economic multipliers that are the aggregate impact of a change in output.

¹⁸ OECD, 2017c.

¹⁹ This means that regardless of why the losses occur, systemic costs in a particular sector (upstream losses at a sector level) can be described as a multiplicative factor of the direct costs (via the Leontief matrix). For example, if there is \$1 of direct costs in utilities, there is \$A in systemic costs (upstream) in transportation, \$B in systemic costs (upstream) in banking, and so on, regardless of whether the damages were caused by a hurricane, a war, a cyber attack, or something else. Thus, when we use direct costs to inform systemic costs, we only need the direct costs and the OECD factors.

Our approach uses the direct costs estimated using the methods in the previous section to model disruptions to the system. These disruptions are the inputs to the input-output model that can be used to estimate the systematic costs from cyber incidents. Using the Leontief inverse matrix, we are able to estimate changes in the sectors linked to the disrupted sector and the magnitude of the “spillover effect” on these other sectors. In addition, we aggregate the impacts to the national level. Our approach can be used for any country for which there is a SAM. The OECD has created both the SAMs and the Leontief inverse matrixes used to construct sector-specific multipliers for at least 60 countries.²⁰

To produce global estimates, there are three potential approaches. First, one could simply aggregate the estimated impacts for all countries. This would provide a lower bound, as there are linkages across countries that are not captured in the input-output models. The second approach would be to use a global CGE that considers the trade patterns that would be affected by supply-chain disruptions that cascade. One of the problems with this second approach is that it would miss linkages that were not typical supply-chain linkages, particularly where multiple countries are affected by a cyber attack on a single entity. The third approach would incorporate these alternative pathways for cascading effects across countries. Because we want to be transparent and accessible to the widest audience, we have opted to use the first approach.

By incorporating the cascading effects through the supply chain, we are expanding the scope of estimates that can be done. Impacts are not isolated to a particular industry but can cascade to multiple sectors, depending on the nature of the attack and the nature of the production process. To estimate a large-scale disruption, such as a widespread disruption to the power grid or an international cloud computing disruption, we would need to develop a much more intricate CGE that would be calibrated outside of just the SAM with a focus on the interconnected cyber vulnerabilities. Additionally, this would necessarily have to be scenario-based rather than simply spanning a range of alternative assumptions. Early work in this area by Lloyd’s for a blackout scenario,²¹ Lloyd’s and Cyence for a cloud computing or operating system attack,²² and Adam Rose²³ estimating the economic impact of large-scale infrastructure disruptions could provide approaches to estimating these large-scale disruptions in the future.

Using the notation of the previous section, let d_{cio} be the direct output costs of cyber attacks on sector i , and z_{cij} be the entry in the i^{th} row and j^{th} column of $(I_n - A_c)^{-1}$. Systemic output costs in sector i (s_{cio}) arising from direct costs to output are

$$s_{cio} = \sum_{j \in I} z_{cij} d_{cio} \quad \forall i \in I, c \in C$$

²⁰ OECD, 2017c.

²¹ Lloyd’s, 2015.

²² Lloyd’s, 2017.

²³ Rose and Wei, 2013; Wing et al., 2016.

Again, assuming sector output costs and GDP costs scale linearly, the systemic costs to sector GDP are $s_{cig} = s_{cio} \frac{w_{ci}G_c}{O_{ci}} \forall i \in I, c \in C$. Furthermore, aggregating sector-level systemic costs allows us to determine the total systematic costs to output and GDP from cyber incidents for each country c as follows:

$$s_{co} = \sum_{i \in I} s_{cio} \text{ and } s_{cg} = \sum_{i \in I} s_{cig} \forall c \in C$$

The total output cost due to cyber risk for each country is the sum of the direct and systemic costs: $d_{co} + s_{co}$. However, aggregating at a global level is less straightforward. That is, aggregating across countries underestimates trade effects while double-counting sector costs and requires an exhaustive country set C . Thus, we provide country-specific cost estimates, which can provide rich insight into global costs.

Projecting Future Costs

Our model allows for the user to update any of the sets or relations between sets for now or in the future. For example, the user could

- assume a constant GDP increase over time
- use the OECD economic forecast data set²⁴ to provide economic forecast summaries for one year of GDP for each country
- alter estimates of how perils (p) will affect financial exposures (e) in the future.

These changes would be propagated through the model to determine new costs. In both cases, the changes can be point estimates or can be drawn from probabilistic distributions, resulting in a distribution of future costs. In our model, we specifically assume that the global forecasts for each sector i are well studied by other academic and industry researchers and can be used to estimate how global sectors may change in the future. We also allow the user to view costs within a country c over a year, with a caveat that these global forecasts may not be country-specific. Our base model makes the simplest assumption and implements a 1-percent increase in GDP each year for high-income countries, a 6-percent increase for upper-middle-income countries, and a 7-percent increase for lower-middle-income countries, based on World Bank classifications.²⁵

²⁴ Example: OECD, 2017b.

²⁵ World Bank, 2016.

Chapter 3: Model Parameters

The previous chapter outlined the model structure implemented in the Excel tool. Many different sets of parameters need to be specified for the model to run. To exercise the model and confirm that results were comparable to those in existing research, we populated the parameter sets using information from reviews of the literature and data analysis. The parameters can be either point estimates or probability distributions, and the tool can provide expected values and probability distributions of outputs.

Sets

Country (C)

Recall that we defined c as a particular country within a set of countries, C . Per the Ponemon Institute reports, the countries and regions currently suffering the most cyber attacks are the United States, the United Kingdom, Germany, Australia, France, Brazil, Japan, Italy, India, Canada, South Africa, the Middle East (e.g., the United Arab Emirates, Saudi Arabia), and countries in the Association of Southeast Asian Nations (e.g., Singapore, Indonesia, Philippines, Malaysia).²⁶ Because our model should be flexible enough to include future countries at risk, we expanded this set to a broader array of countries.

Because the countries are related to the sectors (and this is the only information we need on the countries), we sought a broad data set that included data on how sectors relate to country. Here, we use the best available data on the 63 countries and one region (rest of world) for which the OECD has collected economic information.²⁷ For each country, we collected GDP data in USD2012 and updated the growth in each country and industry sector to convert to GDP in USD2016.

Industry Sectors (I)

Recall that we defined i as a particular industry sector within a set of industry sectors, I . Our sectoring of the economy is based on a custom sectoring using on available country-level data, as well as the incorporation of what Deloitte has described as the most important sectors for cyber attacks.²⁸ The country-level economic data are based on the Structural Analysis Database (STAN).²⁹ We aggregated these sectors to mimic the Deloitte sectors of importance, with two

²⁶ Ponemon Institute, 2017.

²⁷ OECD, 2017a.

²⁸ Deloitte, 2016. Of the studies in our literature review, Deloitte's was the clearest in its assumptions regarding parameters, and its authors shared additional information with us to assist in our analysis. Accordingly, many of the parameter sets we use in our example cases closely match those from the Deloitte study.

²⁹ OECD, 2017d.

minor differences. First, the OECD data set did not have cyber attacks in mind with their sectoring; as such, there are sectors that are aggregates of sectors in the Deloitte sectoring. For example, there is only a single sector in the OECD sectoring that corresponds to banking and asset management and pensions, whereas there are two sectors in the Deloitte data set. Similarly, there is only a single sector that corresponds to telecom and media. Second, the Deloitte sectoring is not exhaustive of the economy. To calculate the systemic costs, we need an additional sector that corresponds to the rest of the economy. We created this other sector by including all sectors that did not have a match to a Deloitte sector.

Financial Exposures (E)

Recall that we defined e as the financial exposure within a set of financial exposures, E , that could possibly be harmed, independent of hazard type. We consider these exposures, not in their direct contribution to GDP, but as an input to production that when damaged by a cyber attack could reduce a firm's total revenue. Following the work of Jacobs, Bulters, and van Wieren,³⁰ we define the set of financial exposures as capital assets, intellectual property (IP), and income. To translate the stock of assets and intellectual property, we consider the stream of production that is tied to it. This allows us to consider it as a proportion of GDP, which is a flow variable.

We expect this set to be modified by researchers. Thus, here we propose a potential set of exposures that will likely be updated. Specifically, we define three subsets of this set as capital assets, IP, and net income:

- *Capital assets* are the physical property held by a firm, such as its land, buildings, machinery, vehicles, and computers. Therefore, we consider the ability of cyber perils to negatively affect capital assets, and thereby reduce their revenue, as a financial exposure of that firm.
- *IP* is the proprietary ideas, designs, recipes, business practices, patents, trademarks, copyrights, and processes that a firm possesses. IP allows firms to distinguish their product from those of other firms, whether protected by formal processes, such as patents and trademarks, or unprotected, such as recipes and processes. Therefore, we consider the ability of cyber perils to reduce a firm's IP (i.e., IP theft), which could reduce firm revenue due to competitive advantages, as a financial exposure of that firm.
- *Net income* is another term for profit. Profit is calculated as total revenue minus total costs. Therefore, we consider potential damage to a firm's profit resulting from a cyber attack as an exposure of that firm.

The limitations of this list include the following:

- This list does not include reputational loss. With regard to "reputational risk," this can be thought of as a loss of a capital asset. At present, we do not break out this aspect separately but will consider how to incorporate and estimate it in the future.
- This list does not explicitly include an individual's time or income. The OECD data do not allow us to disaggregate value added into its component parts, of which income is one. As such, the systemic costs include but do not explicitly state the impact on income.

³⁰ Jacobs, Bulters, and van Wieren, 2016.

Much of the cost data used to calibrate the model come from lawsuits. We can think of these costs as being captured in the settlement. This is a transfer from one agent to another and would thus net out in a systemic cost calculation.

- This list does not calculate costs to an individual; a strength of this approach is a decrease in double counting. Our model explicitly calculates costs to a nation.
- This list does not include wages lost due to a death. The systemic costs can be renormalized to payments to labor and payments to capital, but the OECD data do not disaggregate these two forms of payment. Because we are not calculating loss of life in the current version, we will not be pursuing the role of lost wages due to death.
- This list does not include costs such as those associated to injuries or lives lost. At present, there is no good way to predict loss of life from cyber attacks as a general approach. As such, we will not be pursuing this approach.

Perils (P)

Recall that we defined p as the peril within the set of perils, P , where a cyber attacker's actions on objectives may result in costs realized by the defender. We expect this set to be modified by researchers. Thus, here we propose a potential set that will likely be updated.

Because we are focusing on the economic sectors, we first sought to populate this section using the Advisen categories for event type. The Advisen data set³¹ contains more than 12,000 incidents classified into five separate entries for event type and 11 separate entries for case type. Table 3.1 maps each case type to its most likely event type.

Table 3.1. Advisen Data Set Case Types Mapped to Event Types

Event Type	Case Type
Data breach	Digital data breach, loss, or theft Improper disposal/distribution, loss, or theft (printed records)
Phishing and identity theft	Identity theft/fraudulent use or access Phishing, skimming
Privacy violation	Improper collection of digital data Privacy violations
Security incident	Cyber extortion Denial of service/system disruption Digital asset loss or theft System/network security violation or disruption
Null (other)	Digital breach/identity theft

We note that some cyber incidents, such as cyber warfare, would not be covered by the case types listed here. Other events that might be difficult to fit into this taxonomy are the Sony Pictures hack, the Democratic National Committee hack, the Ukraine electric infrastructure outage, and such situations as a government hacking a technology company and then six months later making similar technology.

³¹ See Advisen (2017) for more information about the Advisen data set.

A second potential way to populate this section is to use the National Institute of Standards and Technology (NIST) *Standards for Security Categorization of Federal Information and Information Systems*,³² the NIST *Guide for Conducting Risk Assessments*,³³ or other standards. These sources characterize threats to the U.S. federal government (both information and information systems) as a function of confidentiality, integrity, and availability. By contrast, for our example cases, we wanted to distinguish between IP and personally identifiable information (PII) theft, which is why we did not use this peril characterization.

We chose to use another method to identify the perils: using the cyber kill chain, developed by Lockheed Martin.³⁴ The phases of the cyber kill chain include reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objective. Rather than explore actions throughout the kill chain, we focus on understanding the final actions on objectives as the point where costs are realized by the defender. We define the following set of mutually exclusive actions on objectives as a list of cyber subperils:

- exfiltration of company data (e.g., internal documents, IP, trade secrets); costs include losses due to copying blueprints or the publication of defamatory information
- exfiltration of customer data (e.g., loss of PII); costs include notification and compensation
- degradation, destruction, and corruption of data and systems, including cyber physical systems, with the potential for loss of human life
- loss of business due to disruption of systems and assets, as well as denial of service attacks; costs reflect friction from business transfer but ideally do not double-count business that is taken to another company, as that money is not lost.

These subperils can be temporary (e.g., a temporary loss of web service) or persistent (e.g., exfiltration occurring over an extended period).

Again, we note that this set will likely be modified by researchers, and we have created the model such that this is easily possible.

Mapping Notable Cyber Incidents to Sets

Next, we consider a representative sample of attacks to demonstrate our methodology. We follow the recent work of Davis et al.³⁵ in listing notable attacks and include updates to emphasize recent events, large private-sector incidents, and fewer government incidents (Table 3.2). For each notable attack, we describe actions on objectives, the specific exposure, and business sector, thereby noting how each fits into our framework for describing cyber costs, as well as those that do not. Notably, significant losses of PII, particularly in the case of the 2015 U.S. Office of Personnel Management and 2017 Equifax exfiltrations, have second-order costs borne by the parties whose PII was lost that are not fully accounted for in our model.

³² NIST, 2004.

³³ NIST, 2012.

³⁴ Lockheed Martin, 2014.

³⁵ Davis et al., 2017.

Additionally, there are increasing concerns about the potential for extreme cyber conflict and cyber warfare. While cyber warfare is an evolving concept, we distinguish between cyber hacks that exfiltrate information and cyber attacks that degrade, destruct, corrupt, and disrupt, where hacks by state actors (i.e., state, state-sponsored, and state-backed) fall under espionage and attacks by state actors fall under warfare. Table 3.2 provides examples of both; the Stuxnet attack against the Iranian nuclear program, the distributed denial of service (DDoS) attack against U.S. banks, the Ukraine power grid attack, the German parliament attack, and the Democratic National Committee attack are widely considered acts of cyber warfare, while the U.S. Office of Personnel Management hack is widely considered an example of espionage.

We emphasize that this approach removes the need to define the point of entry to the system, the kind of attacker, or whether an attack is internal or external. A future model user could update model modules as needed to account for these.

Table 3.2. Perils (p) and Exposures (e) of Notable Cyber Incidents, by Sector (i) and Country (c)

Incident (Country, Date)	Description	Peril	Exposure	Sector
Stuxnet worm (Iran, 2010)	Cyber weapon causing physical destruction of centrifuges used in the Iranian nuclear program	Degradation and destruction of physical systems	Capital assets	Public
DDoS attacks on U.S. banks (USA, 2012)	Denial of service attacks on more than 46 major U.S. financial institutions	Disruption of business	Net income through lost revenue	Banking
Saudi Aramco (Saudi Arabia, 2012 and 2016)	Destruction of 35,000 Saudi Aramco computers in 2012; a similar attack occurred in late 2016	Destruction of data and systems	Capital asset destruction Net income loss from disruption	Oil, gas, and chemicals
Yahoo data breaches (USA, 2013 and 2014)	Exfiltration of more than 500 million user records, including login information	Exfiltration of customer data	Net income through liability and lost revenue	Technology
Sony Pictures (USA, 2014)	Exfiltration and leak of sensitive information and business disruption	Exfiltration of company data	Intellectual property Net income	Media
GitHub (USA, 2015)	Large and persistent denial of service attack on GitHub	Denial of service	Net income	Technology
TV5Monde (France, 2015)	18-hour outage of French TV network TV5Monde	Disruption of business	Net income	Media
Office of Personnel Management (USA, 2015)	Exfiltration of more than 21.5 million highly sensitive PII records.	Exfiltration of customer data	This has no clear mapping to costs in our framework	Public
German parliament (Germany, 2015)	Exfiltration of 2,420 secret files from a German parliament database and WikiLeaks release	Exfiltration of organization data	This has no clear mapping to costs in our framework	Public

Incident (Country, Date)	Description	Peril	Exposure	Sector
Ukraine power grid (Ukraine, 2016)	Attack disrupting service of Ukrainian energy distributors, cutting power to 225,000 customers	Business disruption and denial of service	Direct cost in net income of utilities and systemic cost in net income of users	Utilities
Democratic National Committee (USA, 2016)	Exfiltration of campaign documents and presidential election interference	Exfiltration of organization data	This has no clear mapping to costs in our framework	Public
Bangladesh Central Bank (Bangladesh, 2016)	Attack leading to an \$81 million heist from the Bangladesh Central Bank	Corruption of data and systems	Loss of \$81 million in assets	Public
Mossack Fonseca (Panama, 2016)	Significant data exfiltration leading to 11.5 million leaked documents representing hundreds of thousands of offshore entities	Exfiltration of customer data	Direct costs include loss of IP and net income; systemic costs include loss in client net income	Business and professional services
Dyn (USA, 2016)	Denial of service attack on domain name service provider Dyn, leading to disruptions for a significant number of customer websites	Denial of service	Direct costs to Dyn's net income and systemic costs to net income of customers	Technology
notPetya (global, 2017)	Ransomware attack beginning in Ukraine leading to major disruptions in shipping, advertising, and pharmaceuticals worldwide	Business disruption and destruction of data and systems	Net income losses borne through business interruptions	All
WannaCry (global, 2017)	Ransomware attack leading to major disruptions at hospitals, universities, and business worldwide	Business disruption and destruction of data and systems	Net income losses borne through business interruptions	All
Equifax (USA, 2017)	Loss of 143 million sensitive U.S. PII records	Exfiltration of customer data	Net income loss to Equifax; full PII costs not captured in model	Business and professional services

NOTE: Most of the incidents are described in Davis et al., 2017; notPetya is described in Thompson, 2017.

Relations Between Sets

Country-Specific Sector Weights (w_{ci})

Recall that we defined w_{ci} as the unitless fraction of the country's GDP that is in sector i . Thus, $w_{ci} * G_c$ represents the GDP of country c that is in sector i . We characterize sectors within a country using the OECD data set for the percentage that each sector contributes to GDP.³⁶ We can additionally collect the output by sector for each of these countries (O_{ci}) from the OECD data.

³⁶ OECD, 2017c.

Sector-Exposure Relationship (Y_{cie})

Recall that we defined the unitless value Y_{cie} as the fraction of the quantity $w_{ci} * G_c$ that is equivalent to the amount of money at risk from each exposure type (e), regardless of whether they can be harmed by a cyber attack. Note that the summation of Y_{cie} across e for a particular c and i is not equal to 1.

We expect this relationship to be modified by researchers. We propose two potential sector-exposure relationships (or “modules”). For both modules, we make the simplifying assumption that GDP per sector and revenue per sector scale, thus allowing us to use revenue as a basis for the calculation. We anticipate that these modules will provide different results, and, thus, we provide both modules to the user to help characterize the deep uncertainty associated with this table.

Module Y1: Dutch Sector-Exposure Estimates

In Module Y1 (Dutch Sector-Exposure Estimates), we use existing literature to characterize this table. Specifically, research by Jacobs, Bulters, and van Wieren³⁷ investigates financial sheets from approximately 50 Dutch companies and defines a relationship between financial exposures (e) and company revenue as given in Table 3.3.

Table 3.3. Module Y1: Dutch Sector-Exposure Relationship (Y_{cie}) as Given in Literature, Unitless

Sector Exposure	Capital Assets	Intellectual Property	Net Income
Asset management and pensions	U(0,0)	U(0,0.03)	U(0,0.03)
Banking	U(0,0)	U(0.01,0.05)	U(0,0.5)
Business and professional services	U(0,0)	U(0,0)	U(0.02,1)
Consumer goods	U(0.02,0.06)	U(0.01,0.08)	U(0,0.1)
Defense and aerospace	U(0.25,1)	U(0.4,1)	U(0,1)
Health care and insurance	U(0,0)	U(0.003,0.02)	U(0,0.13)
Media	U(0.02,0.06)	U(0.01,0.04)	U(0,0.05)
Oil, gas, and chemicals	U(0,0.0004)	U(0.02,0.13)	U(0,0.13)
Public	U(0,0.002)	U(0,0.03)	U(0,0.1)
Technology and electronics	U(0.02,0.06)	U(0.01,0.04)	U(0,0.38)
Telecom	U(0.1,0.4)	U(0.01,0.04)	U(0.02,0.5)
Transportation	U(0,0.01)	U(0,0.003)	U(0,0.05)
Utilities	U(0,0.01)	U(0.003,0.02)	U(0,0.05)
Wholesale and retail	U(0,0.01)	U(0.003,0.02)	U(0,0.05)
Other	0	0	0

NOTE: U(a,b) indicates a uniform distribution from a to b .

This relationship includes expert information on exposures that could not be affected by cyber attacks (e.g., a cornfield would be excluded) and cyber defenses or controls that might be employed by the sector (e.g., antivirus software would be included). We assume that the sectors not mentioned in Jacobs, Bulters, and van Wieren are not affected by cyber attacks; to represent this in our model, we set these values to 0. A caveat with this module is that a particular Y_{cie} entry may be a function of only one or two companies that may not represent a large percentage

³⁷ Jacobs, Bulters, and van Wieren, 2016.

of the market share of that industry. Thus, we can interpret Module Y1 as the fraction of revenue in each sector that is equivalent to the amount of money represented by each exposure type e and can be harmed by a cyber attack.

Module Y2: U.S. Securities and Exchange Commission Sector-Exposure Estimates

In Module Y2 (SEC Sector-Exposure Estimates), we estimate the sector-exposure relationship Y_{cie} , using financial data from publicly traded companies. Unlike Module Y1, we do not incorporate expert knowledge, and thus Module Y2 includes all exposures, regardless of whether they could be affected by cyber attacks (e.g., a cornfield would be included) and does not include cyber defenses or controls that might be employed by the sector (e.g., antivirus software would be excluded). Thus, we can interpret Module Y2 as the fraction of revenue in each sector that is equivalent to the amount of money represented by each exposure type e , regardless of whether it can be harmed by a cyber attack; Module Y2 is the upper bound on the exposures that could possibly be damaged.

The estimation of Y2 is intended to add transparent rigor to the analysis of potential cyber costs to the economy. While we draw inspiration from the Jacobs, Bulters, and van Wieren³⁸ analysis using income, assets, and IP as inputs, each term is slightly ambiguous. For example, *income* may refer to net income, gross income, revenue, or value added, each with a significantly different meaning. Furthermore, it is unclear whether prior efforts have aimed to model firm valuation or value added. Acknowledging a potential difference in interpretation, we clarified our definitions of the three independent variables as net income, total assets, and spending on research and development (R&D; used as a proxy for IP), with revenue as the dependent variable, and collected data on each for 4,447 publicly traded firms from firm income statements, cash flow statements, and balance sheets filed in 2013, 2014, 2015, and 2016.³⁹ Furthermore, given the assumption that valuations are based on outputs, effectively making sector valuation equal to sector output, the two potentially different approaches are directly comparable. To estimate the relationship Y_{cie} , we analyzed the impact of each exposure on revenue and then made the simplifying assumption that GDP per sector and revenue per sector scale linearly. This allows us to greatly simplify the regression and use GDP (which represents percentage change of revenue) as a basis of the calculation; a more complicated analysis could include an extra step of directly relating the revenue of each company to the sector's GDP.

We estimate the impact of net income, total assets, and R&D (IP) on revenue as an elasticity by sector specific in the equation below. Taking logarithms of dependent and independent variables in the regression, each coefficient has the interpretation of a percentage change in exposure resulting in a percentage change in revenue. Thus, the regression estimates that a 1-

³⁸ Jacobs, Bulters, and van Wieren, 2016.

³⁹ Firm balance sheets, income statements, and cash flow documents are publicly available from SEC 10-K filings.

percent change in total assets for a given firm in sector i , for example, results in β_3 a-percent change in total revenue:

$$\log(\text{Revenue}_i) = \beta_1 \log(\text{R\&D}_i) + \beta_2 \log(\text{NetIncome}_i) + \beta_3 \log(\text{TotalAssets}_i) + \epsilon \quad \forall i \in I$$

Coefficients β_i are therefore multiplier effects associated with each financial exposure. Thus, if $\beta_i = 0$, exposure i has no impact on revenue; if $0 < \beta_i < 1$, the exposure has a weak impact on revenue; if $\beta_i = 1$, exposure i leads to a 100-percent transfer of revenue; and if $\beta_i > 1$, exposure i has a magnified effect on revenue. Therefore, given an elasticity of 0.9 ($\beta_3 = 0.9$) for total assets, we expect a cyber attack leading to 1-percent, 10-percent, and 100-percent asset losses to cause 0.9-percent, 9-percent, and 90-percent losses in revenue, respectively.

The above relationship was estimated using ordinary least squares regression for each sector. Table 3.4 displays the coefficients, number of observations, and fit for each sector-specific regression, including a regression with all sectors. The regression makes two notable limiting assumptions. First, the regression assumes that the results can be interpreted causally rather than descriptively. Second, the regression assumes that R&D is correlated to *current* period intellectual property. Assuming that results can be causally interpreted, the regression outputs for all sectors imply that a 1-percent change in R&D leads to a 0.02-percent change in revenue, that a 1-percent change in net income leads to a 0.04-percent change in revenue, and that a 1-percent change in total assets leads to a 0.92-percent change in revenue. Notably, all sectors except for health care and insurance have strong model fits. After taking logarithms of each exposure, the health care and insurance sector is left with an insufficient number of observations to provide an accurate fit by regression.

Table 3.4 shows fitted coefficient values for sector-specific regressions estimating the above equation, along with associated numbers of observations and R^2 values. The health care and insurance sector was dropped due to insufficient data. Appendix C contains the full regression output.

To apply the fitted coefficients in Table 3.4 to Y_{cie} , two key adjustments are required. To fit the assumptions of our model, we truncate coefficients such that $\beta_i \geq 0$. Second, each coefficient in Table 3.4 is a point estimate, and providing a confidence interval around each is necessary to reflect uncertainty. Consequently, we express Y_{cie} in Table 3.5 by providing a 95-percent confidence interval (calculated using coefficient standard errors from each regression) truncated at 0. Furthermore, while we were unable to estimate the health care and insurance sector by regression, we artificially impose the results of the “other” sector to provide general insight.

We note that this analysis appears to suggest that almost all revenue is driven by assets. It is not that surprising that revenue and assets are very strongly correlated, with larger companies having more assets and more revenue. R&D, by contrast, is an investment that does not necessarily need to scale with company size. For example, consider two pharmaceutical companies, one that specializes in “blockbuster” drugs and another that focuses on less common

diseases. They could easily spend similar amounts on R&D and have vastly different revenue, and loss of IP could be devastating for both, even if R&D is not strongly correlated with revenue. In addition, R&D may have time lags that would not be apparent in this sort of analysis or may not be disclosed in the SEC files. Thus, we strongly caution the user against considering these correlations to be causations.

The estimated values of Y_{cie} convey that R&D has generally weak impacts on revenue, while total assets have the strongest impact. In fact, most intervals on $Y_{ci,R\&D}$ include the value 0, implying that R&D (and, therefore, IP) may, in some cases, have no impact. In comparison, $Y_{ci,Total\ Assets}$ is centered near the value 1 for most sectors and, at times, even exceeds the value 1, implying that total assets have the potential for a magnified impact on revenue in many sectors. Thus, cyber attacks with the potential to damage assets will result in the highest direct costs for most sectors. A notable exception elucidates a key vulnerability with a potential for high costs; the utilities sector carries significant uncertainty on the impact of IP (R&D) and net income, where losses in either range from no impact to magnified impacts on revenue.

Table 3.4. Results of Sector-Exposure Regression, Unitless

Sector	R&D	Net Income	Total Assets	Observations	R^2
All sectors	0.02	0.04	0.92	2,958	0.9943
Banking	0.06	-0.04	0.88	28	0.9909
Business and professional services	0.16	0.02	0.82	137	0.9877
Consumer goods	-0.06	0.05	0.96	1,012	0.9960
Health care and insurance	-	-	-	-	-
Oil, gas, and chemicals	0.17	0.16	0.72	141	0.9966
Public	-0.12	0.15	0.91	15	0.9976
Technology and electronics	0.00	0.02	0.95	194	0.9949
Telecom	0.14	-0.05	0.89	299	0.9897
Transportation	-0.19	-0.02	1.08	12	0.9984
Utilities	0.66	0.11	0.61	9	0.9949
Other	-0.03	0.07	0.93	1,035	0.9953

NOTE: Some sectors are not included due to insufficient data.

Table 3.5. Module Y2: SEC Sector-Exposure Relationship (Y_{cie}), Unitless

Sector Exposure	Capital Assets	Intellectual Property	Net Income
Asset management and pensions	U(0.91, 0.93)	U(0, 0.03)	U(0.02, 0.05)
Banking	U(0.75, 1.01)	U(0, 0.31)	U(0, 0.18)
Business and professional services	U(0.75, 0.9)	U(0.05, 0.28)	U(0, 0.12)
Consumer goods	U(0.94, 0.98)	0	U(0.02, 0.07)
Defense and aerospace	U(0.91, 0.93)	U(0, 0.03)	U(0.02, 0.05)
Health care and insurance	U(0.91, 0.93)	U(0, 0.03)	U(0.02, 0.05)
Media	U(0.91, 0.93)	U(0, 0.03)	U(0.02, 0.05)
Oil, gas, and chemicals	U(0.67, 0.78)	U(0.12, 0.22)	U(0.07, 0.25)
Public	U(0.81, 1.0)	U(0, 0.09)	U(0, 0.34)
Technology and electronics	U(0.9, 0.99)	U(0, 0.09)	U(0, 0.09)
Telecom	U(0.84, 0.94)	U(0.07, 0.21)	U(0, 0.01)
Transportation	U(0.9, 1.3)	0	U(0, 0.33)
Utilities	U(0, 1.4)	U(0, 1.4)	U(0, 1.2)
Wholesale and retail	U(0.91, 0.93)	U(0, 0.03)	U(0.02, 0.05)
Other	U(0.91, 0.93)	U(0, 0.03)	U(0.02, 0.05)

NOTE: U(a,b) indicates a uniform distribution from a to b.

Exposure-Peril Relationship (X_{ciep})

Recall that we defined the unitless value X_{ciep} to be the fraction of the exposure at risk in country c and sector i and exposure type e that will be successfully destroyed, stolen, or otherwise lost due to a particular peril p . We expect this relationship to be modified by researchers. Thus, here we propose two potential relationships (i.e., modules). Although the model allows entering peril-exposure estimates by country and industry sector, due to limitations in available data, we were unable to distinguish the exposure-peril relationship by industry sector. For the examples shown in this document, we assume that X_{ciep} is constant across sectors and thus characterize it as X_{cep} . We anticipate that researchers with other data or modeling assumptions will be able to fully flesh out these estimates across industry sectors. We note that these modules will provide different results, and thus we provide both to the user to help characterize the deep uncertainty associated with this table. In addition, if the user would like to create alternative modules, we have provided Appendixes E and F as potential guides.

Module X1: Dutch Peril-Exposure Estimates

In Module X1 (Dutch Peril-Exposure Estimates), we create a reduced-form model⁴⁰ based on a literature review. Here, we used Deloitte (2016) and mapped to our taxonomy. Specifically, we mapped as shown in Table 3.6 and obtained Table 3.7. Note that due to the assumptions in the mapping and the fact that Deloitte does not capture many of the costs associated with our peril taxonomy, Module X1 identifies the same values for (1) the two types of exfiltration and (2) the other two types of perils.

Table 3.6. Mapping Deloitte's Threats to Our Model Perils

Deloitte's Threats	Model Perils			
	Exfiltration of Company Data	Exfiltration of Customer Data	Data Degradation, Destruction, and Corruption	Disruption of Business and Denial of Service
Cyber physical			X	
Data breach	X	X		
Data destruction or wipe			X	X
Malware	X	X		X
Ransomware	X	X		X
Sabotage			X	X

⁴⁰ A reduced-form model is created by rearranging a set of equations so that all endogenous variables are dependent variables. Here, we use a combination of a reduced-form model (solving for endogenous variables) and dimension reduction (removing components of cyber defenses) to provide a set of parameters describing this relation.

Table 3.7. Module X1: Dutch Peril-Exposure Relationship (X_{cep}), Unitless

Threat Exposure	Capital Assets	Intellectual Property	Net Income
Exfiltration of company data	T(0,0.0043,0.021)	T(0,0.00012,0.00096)	T(0,0.0015,0.0032)
Exfiltration of customer data	T(0,0.0043,0.021)	T(0,0.00012,0.00096)	T(0,0.0015,0.0032)
Data degradation, destruction, and corruption	T(0,0.0083,0.041)	T(0,0.00025,0.0021)	T(0,0.0031,0.0079)
Disruption of business and denial of service	T(0,0.0083,0.041)	T(0,0.00025,0.0021)	T(0,0.0031,0.0079)

NOTE: T(a,b,c) indicates a triangular distribution where a is the minimum value, b is the mode, and c is the maximum value.

Alternative Method for Directly Estimating Potential Economic Damage

We seek to estimate the potential direct costs associated with cyber incidents. Similar to the concept of value at risk (VaR) used in finance and insurance models, our objective is to measure potential economic damage rather than predict the level of damage in any given year. That is, we aim to provide a high-level estimate which, while only met in the extremes, provides insight into the total risk to the economy at large presented by cyber incidents.

To measure the direct cost potential of a given country, we use sector-specific data on prior revenues and costs. The Advisen data set, which includes descriptions of cyber incidents from 2005 to 2015 in the United States (see Appendix D), can be used to determine costs incurred as a result of cyber incidents in each sector. While significant uncertainties surrounding the impact of cyber incidents and relatively sparse data prevent the data set from capturing the full distribution of costs, it can provide insight into the potential range of costs.

Using the Advisen data set, we estimated the cost of cyber attacks on each sector as a fraction of sectoral revenue. To do so, we used incident-level data to construct a sample of cost per revenues. However, knowing that this sample is only a portion of a much larger population of incidents, we bootstrap resampled the data breach costs from 2005 to 2014 to get a more accurate estimate of possible future cost distributions (2015 incidents appeared to have been logged midyear, so this year was omitted). We created 100,000 new data sets via resampling with replacement by first randomly selecting a number of incidents from the set of incidents per year in said sector and then randomly selecting the data breach costs for said incidents from the set of incident costs in the sector and summed the total data breach costs in the resampled year. We then estimated cost percentiles from the resulting set of 100,000 resamplings to determine the 25th-percentile, 50th-percentile, 75th-percentile, and 95th-percentile direct costs for each sector ($d_{USA,i,\%}$, Table 3.8).

Next, potential direct sector costs can be aggregated to estimate potential direct economic costs. To do so, we use the country-specific sector weights $w_{USA,i}$ and the estimated direct sector costs as a percentage of revenue $d_{USA,i,\%}$ to estimate the potential direct output costs as a fraction of GDP, $d_{USA,\%}$, as follows: $d_{USA,\%} = \sum_{i \in I} w_{USA,i} d_{USA,i,\%}$

Table 3.8. 25th-, 50th-, 75th-, and 95th-Percentile Bootstrapped Values of Direct Costs in the United States for Each Sector as a Percentage of Revenue ($d_{USA,i,\%}$)

Sector	Cost per Revenue Percentile			
	25th	50th	75th	95th
Banking	0.01%	0.04%	0.06%	0.26%
Business and professional services	1.31%	10.66%	31.55%	214.89%
Consumer goods	0.07%	1.29%	5.52%	192.78%
Health care and insurance	0.09%	0.43%	0.77%	10.27%
Public	0.02%	0.09%	0.17%	1.47%
Telecom	0.02%	0.08%	0.26%	25.00%
Transportation	0.01%	2.09%	5.83%	142.88%
Wholesale and retail	0.01%	0.11%	0.33%	3.02%
Oil, gas, and chemicals*	0.17%	1.54%	2.97%	67.69%
Utilities*	0.17%	1.54%	2.97%	67.69%
Other	0.17%	1.54%	2.97%	67.69%

NOTE: Some sectors are not included due to insufficient data.

* Due to an insufficient amount of data on the oil, gas, and chemicals and utilities sectors, we have applied bootstrapped values for the "other" sector to carry calculations through.

Table 3.9. Sector Output Weights for the United States ($w_{USA,i}$)

Sector	Share of GDP
Banking	8.51%
Business and professional services	11.08%
Consumer goods	4.11%
Health care and insurance	7.76%
Public	9.58%
Telecom	2.84%
Transportation	4.09%
Wholesale and retail	10.40%
Oil, gas, and chemicals	2.86%
Utilities	1.86%
Other	23.43%

NOTE: Some sectors are not included due to insufficient data.

To illustrate this calculation, consider an estimation of direct costs in the United States as an example. Table 3.9 shows the sector-output weights, $w_{USA,i}$. Using the values in Table 3.8 and Table 3.9, we estimate the direct costs as a percentage of total GDP in Table 3.10.

To implement this in the model, we would convert Table 3.8 into Tables 3.11 and 3.12 to create VaR direct estimates (X_{cep} = Module X3, Y_{cie} = Module Y3).

There are two caveats to this approach. First, the data are voluntarily reported and mostly relate to data breaches. Other events (both those not reported and significantly different types of events) might be significant. For example, we found relatively low impact in the retail sector, even though we know (via Table 3.2) that the retail sector has been the target of multiple successful cyber attacks. Second, the data are historical and will thus underweigh perils that are only just now manifesting themselves (such as the 2017 notPetya and WannaCry ransomware attacks). In addition, these data fail to capture new types of attacks that have yet to be imagined.

Table 3.10. Determination of U.S. GDP at Risk Using Bootstrapped Values of Direct Costs in the United States for Each Sector as a Percentage of Revenue

	Percentile			
	25th	50th	75th	95th
Direct cost (% of GDP)	0.2%	1.7%	4.8%	55.4%
Total direct cost	\$ 27.8 billion	\$241.9 billion	\$665 billion	\$7.71 trillion

Table 3.11. Module 3: Value at Risk Exposure-Peril Relationship (X_{cep}), Unitless

Threat Exposure	Capital Assets	Intellectual Property	Net Income
Exfiltration of company data	1	0	0
Exfiltration of customer data	0	0	0
Degradation, destruction, and corruption	0	0	0
Disruption of business and denial of service	0	0	0

Table 3.12. Module 3: Value at Risk Sector-Exposure Relationship (Y_{cie}), Unitless

Sector Exposure	Capital Assets	Intellectual Property	Net Income
Asset management and pensions	T(0.0023,0.0023,0.12)	0	0
Banking	T(0.00017, 0.00017,0.031)	0	0
Business and professional services	T(0.012,0.012, 1.97)	0	0
Consumer goods	T(0.0017,0.0017, 0.80)	0	0
Defense and aerospace	T(0.0023,0.0023, 0.12)	0	0
Health care and insurance	T(0.00032,0.00032, 0.033)	0	0
Media	T(0.0023,0.0023,0.12)	0	0
Oil, gas, and chemicals	0.26	0	0
Public	T(0.000083,0.000083, 0.0082)	0	0
Technology and electronics	T(0.0023,0.0023,0.12)	0	0
Telecom	T(0.00013, 0.00013, 0.068)	0	0
Transportation	T(0.000049, 0.000049, 0.047)	0	0
Utilities	T(0.0014,0.0014, 0.15)	0	0
Wholesale and retail	T(0.000079, 0.000079, 0.035)	0	0
Other	T(0.0023, 0.0023, 0.12)	0	0

NOTE: T(a,b,c) indicates a triangular distribution where a is the minimum value, b is the mode, and c is the maximum value.

Chapter 4: Case Studies

There have been many high-profile cyber attacks in recent years, as well as fictional case studies that are based on what might be considered canonical risks in the field. Because of their familiarity, it is natural to ask how our model would represent these specific cases, both in terms of comparing the results of the model and in probing the model's strengths and weaknesses in expressing the scenarios. In some cases, the top-line total economic impact will be relevant—particularly when there is another competing estimate against which it can be benchmarked. We anticipate that this first iteration will track other work reasonably well with some previous estimates but that it may also deviate significantly from others. In either case, the transparency of our model and the possibility for others to subsequently modify or extend it will allow researchers to explore root causes of the discrepancies and motivate further inquiry.

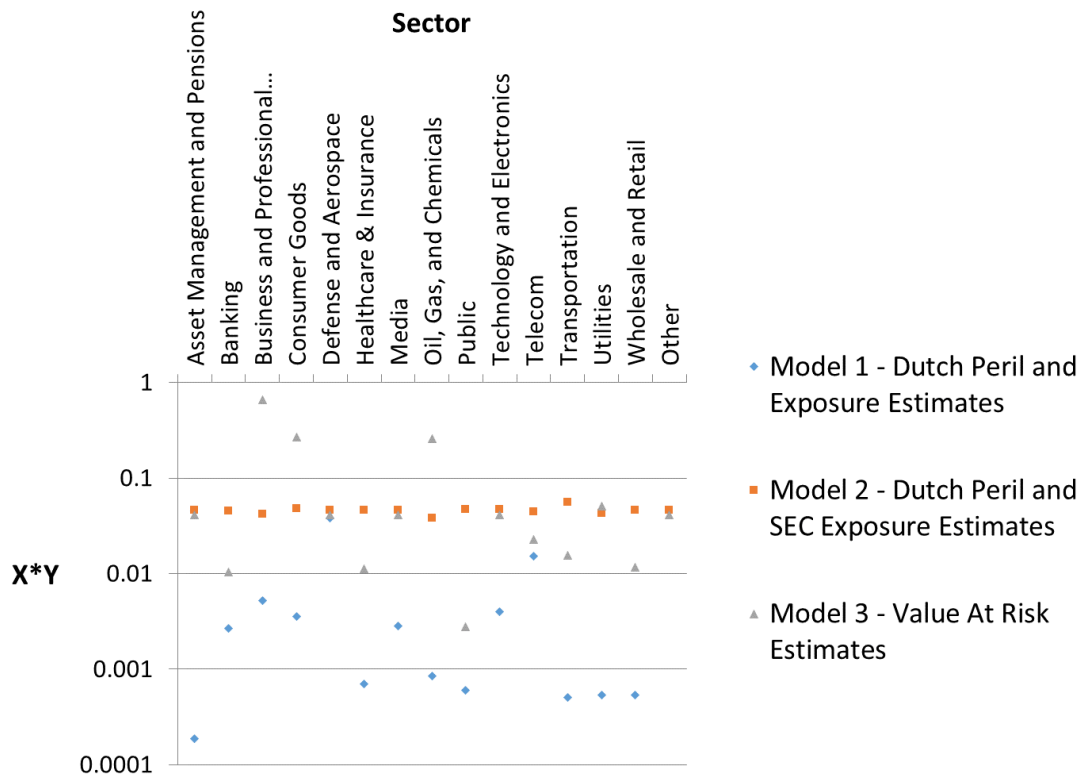
Here, we explore multiple case studies for the different models. We use the different modules and define three models:

- Model 1: Dutch Peril-Exposure and Sector-Exposure Estimates (X_{cep} = Module X1, Y_{cie} = Module Y1)
- Model 2: Dutch Peril-Exposure and SEC Sector-Exposure Estimates (X_{cep} = Module X1, Y_{cie} = Module Y2)
- Model 3: VaR Direct Estimates (X_{cep} = Module X3, Y_{cie} = Module Y3).

As described in Chapter 3, each of these combinations of X_{cep} and Y_{cie} stems from markedly different assumptions and, thus, will produce very different results. To aid in understanding the differences in the results, we have used the expected values for each module, multiplied by X_{cep} and Y_{cie} summing over all financial exposures and perils, to obtain the fractional multipliers to sector output (Figure 4.1). Setting aside magnitude, there are some differences between sectors; Model 1 reports its largest fraction for defense and aerospace, Model 2 for transportation, and Model 3 for business and professional services. These differences are propagated through the resulting calculations and, depending on the amount of GDP in each economic sector, may be minimized or magnified. For example, because the asset management and pensions sector and the media sector do not map to any GDP in our model, the differences between models in the fractional multiplier do not matter.

Now let us explore multiple case studies. Some, such as the global cost of cyber crime or the cost of cyber crime in the Netherlands, build on the strengths of our model to allow for an improved understanding of annual impacts. Others, such as Lloyd's business blackout, demonstrate how our model may be applied to specific extreme events. Table 4.1 provides a summary of the results; the following text gives more complete results.

Figure 4.1. Comparison of Models 1, 2, and 3



NOTES: The vertical axis ($X*Y$) is summed over all exposures and perils, representing the fractional direct impact on the output of each industry sector. The vertical axis is log-scaled.

Table 4.1. Summary of Case Study Results for Different Models

Case Study	Literature	Model 1: Dutch Peril and Exposure Estimates	Model 2: Dutch Peril and SEC Estimates	Model 3: VaR Direct Estimates	Model Implementation of Lloyd's Study
1. Global cost of cyber crime	See Chapter 1	Direct: \$275 billion Total: \$799 billion (1.1% of global GDP)	Direct: \$3.2 trillion Total: \$10.1 trillion (14.5% of global GDP)	Direct: \$6.6 trillion Total: \$22.5 trillion (32.4% of global GDP)	N/A
2. Cost of cyber crime in the Netherlands	1.5% of Dutch GDP	Direct: \$3.4 billion Total: \$9.9 billion (1.26% of Dutch GDP)	Direct: \$35.9 billion Total: \$113.8 billion (14.6% of Dutch GDP)	Direct: \$84.1 billion Total: \$291.3 billion (37.3% of Dutch GDP)	N/A
3. Lloyd's business blackout	\$243 billion to \$1.024 trillion, depending on scenario	N/A	N/A	N/A	Direct: \$184 billion Total: \$515 billion

Global Cost of Cyber Crime

Recall that Chapter 1 contains a literature review on different methods to calculate the global cost of cyber crime. Here, we run the model for the global cost of cyber crime using the default values in the model.

- Model 1: Dutch Peril and Exposure Estimates. Direct GDP losses are \$275 billion, and total GDP losses are \$799 billion (1.1 percent of global GDP); see Figure 4.2.
- Model 2: Dutch Peril and SEC Exposure Estimates. Direct losses are \$3.2 trillion, and total losses are \$10.1 trillion (14.5 percent of global GDP); see Figure 4.3.
- Model 3: VaR Estimates. Direct losses are \$6.6 trillion, and total losses are \$22.5 trillion (32.4 percent of global GDP); see Figure 4.4.

Note that Model 2 has the majority of costs in the “other” category. This occurs due to our definition of Module Y2. Recall that we can interpret Module Y2 as the fraction of revenue in each sector that is equivalent to the amount of money represented by each exposure type e , regardless of whether it can be harmed by a cyber attack; Module Y2 is the upper bound on the exposures that could possibly be damaged.

Figure 4.2. Cost of Global Cyber Crime, Model 1: Breakout of Damages by Sector

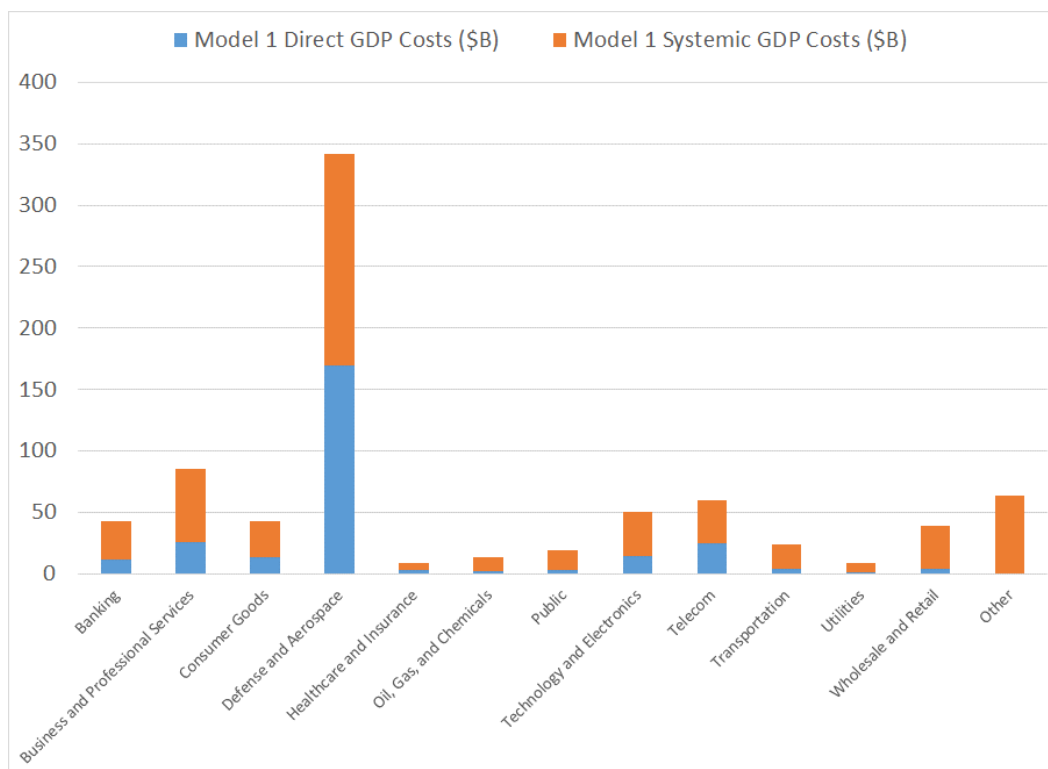


Figure 4.3. Cost of Global Cyber Crime, Model 2: Breakout of Damages by Sector

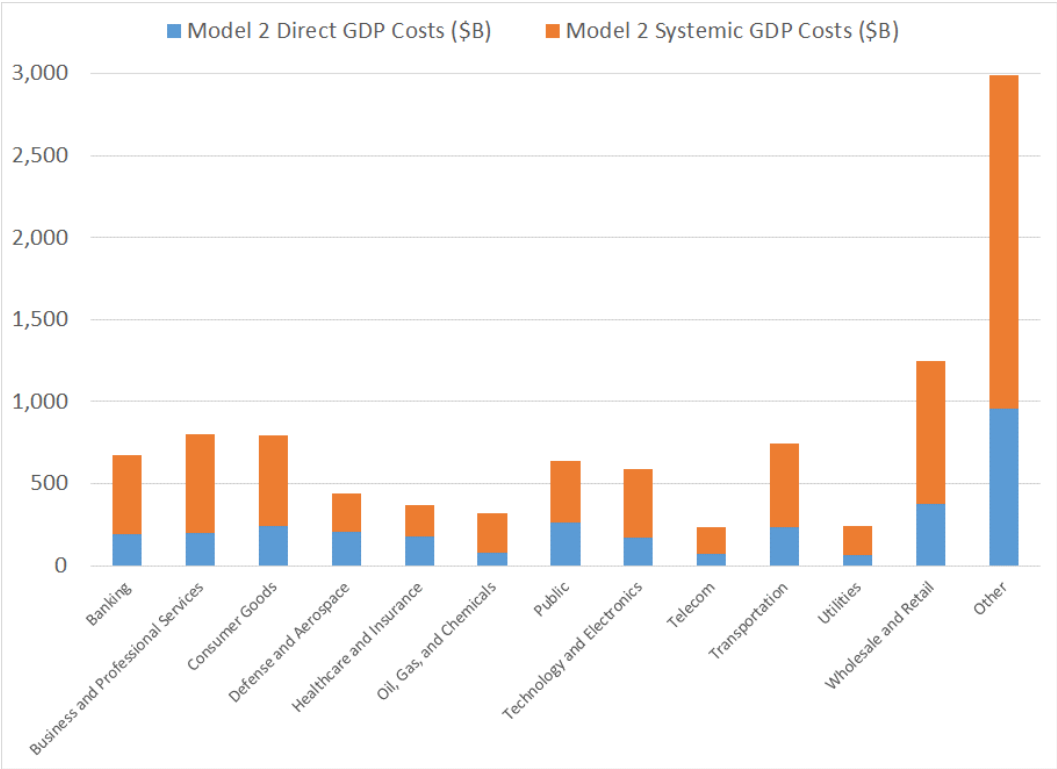
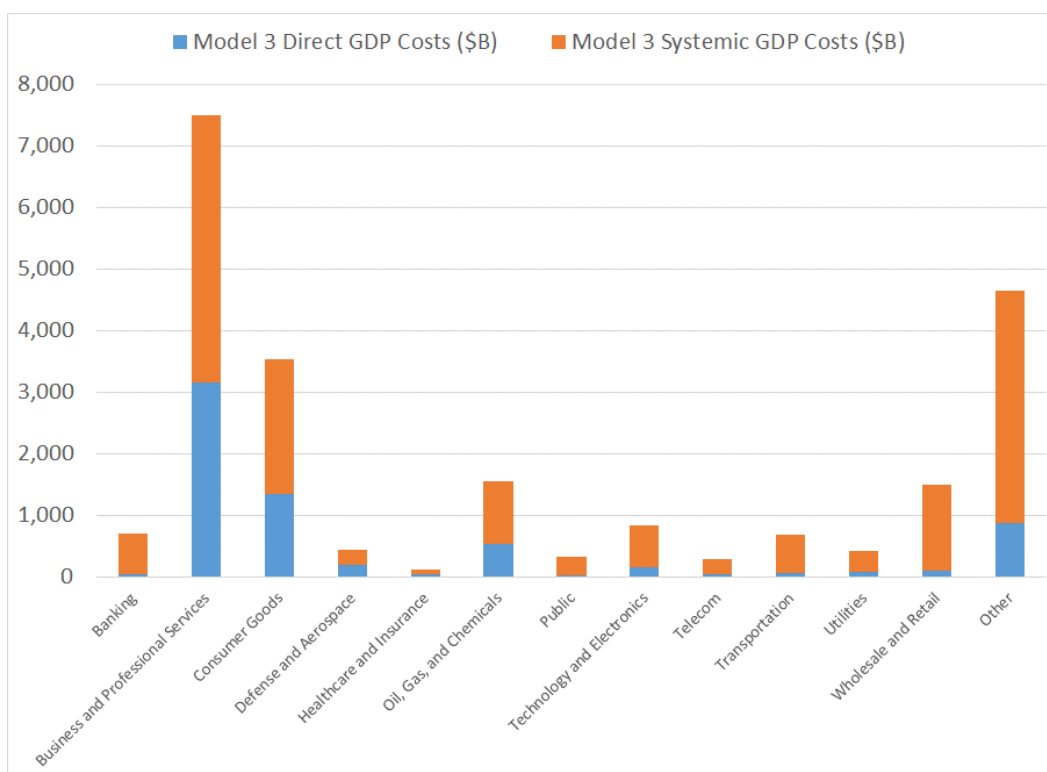


Figure 4.4. Cost of Global Cyber Crime, Model 3: Breakout of Damages by Sector



Cost of Cyber Crime in the Netherlands (1.27 Percent of GDP)

Next, we ran the model for the cost of cyber crime in the Netherlands, which has been estimated to be 1.5 percent of the Netherlands GDP.⁴¹ We assumed base inputs. We found the following:

- Model 1: Dutch Peril and Exposure Estimates. Direct GDP losses are \$3.4 billion, and total GDP losses are \$9.8 billion (1.26 percent of Netherlands GDP); see Figures 4.5 and 4.6.
- Model 2: Dutch Peril and SEC Exposure Estimates. Direct GDP losses are \$35.9 billion, and total GDP losses are \$113.8 billion (14.6 percent of Netherlands GDP); see Figures 4.7 and 4.8.
- Model 3: VaR Estimates. Direct GDP losses are \$84.1 billion, and total GDP losses are \$291.3 billion (37.3 percent of Netherlands GDP); see Figures 4.9 and 4.10.

We specifically note that Model 1 (which was created for this scenario) appears to align well with values predicted by the literature, increasing our confidence in using this model.

⁴¹ Deloitte, 2016.

Figure 4.5. Cost of Cyber Crime in the Netherlands, Model 1: Distribution of Total GDP Costs

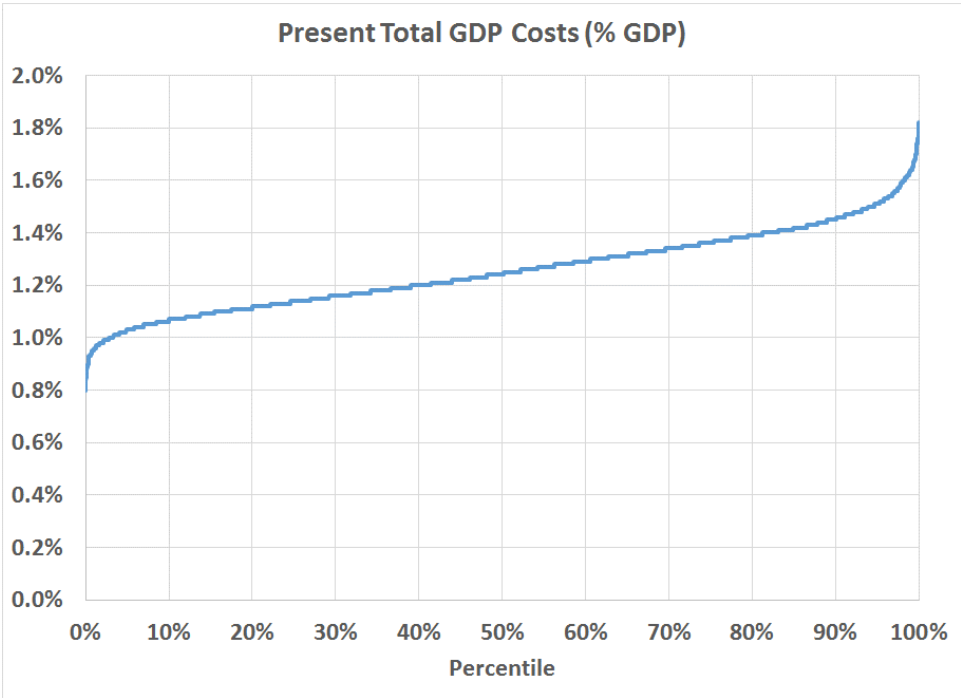
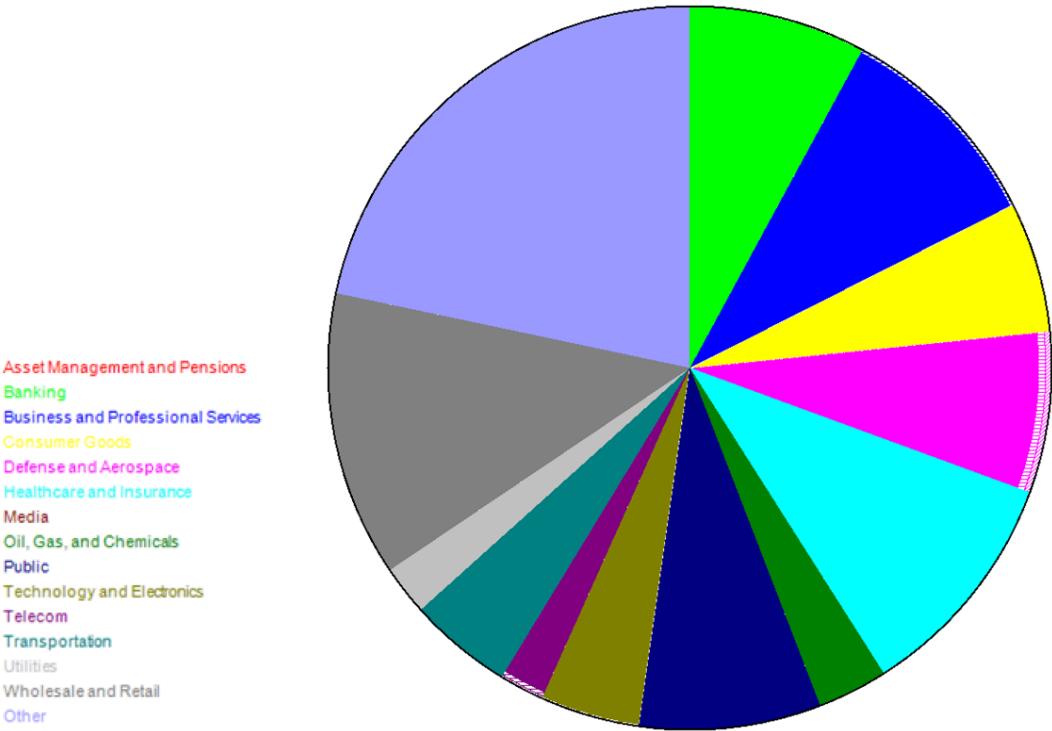


Figure 4.6. Cost of Cyber Crime in the Netherlands, Model 1: Breakout of Damages by Sector



NOTE: Horizontal shaded regions at outer edge denote systemic losses, and solid regions at center denote direct losses.

Figure 4.7. Cost of Cyber Crime in the Netherlands, Model 2: Distribution of Total GDP Costs

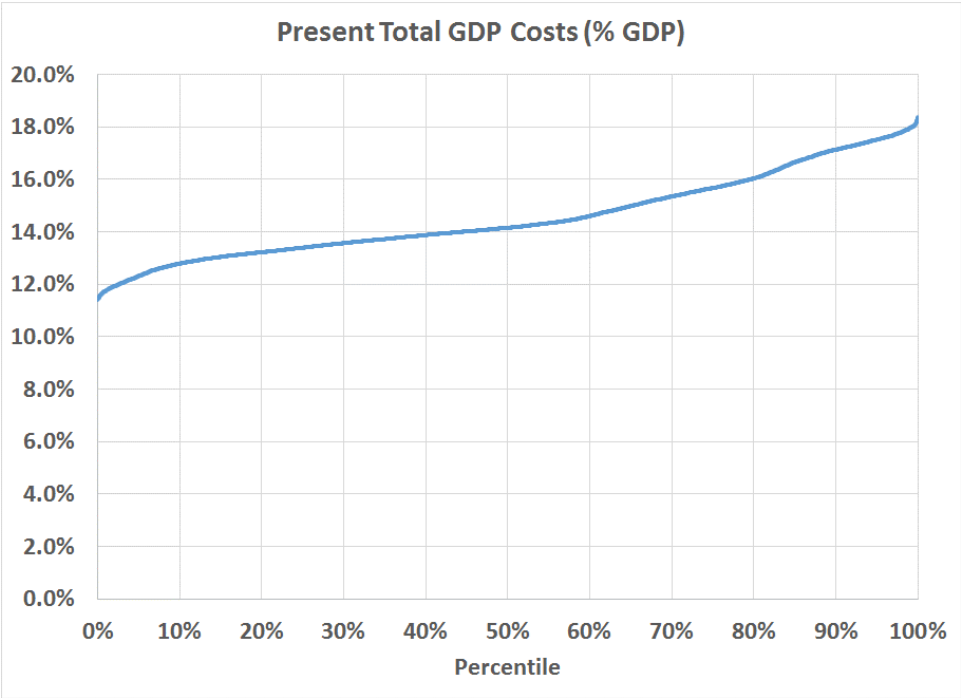
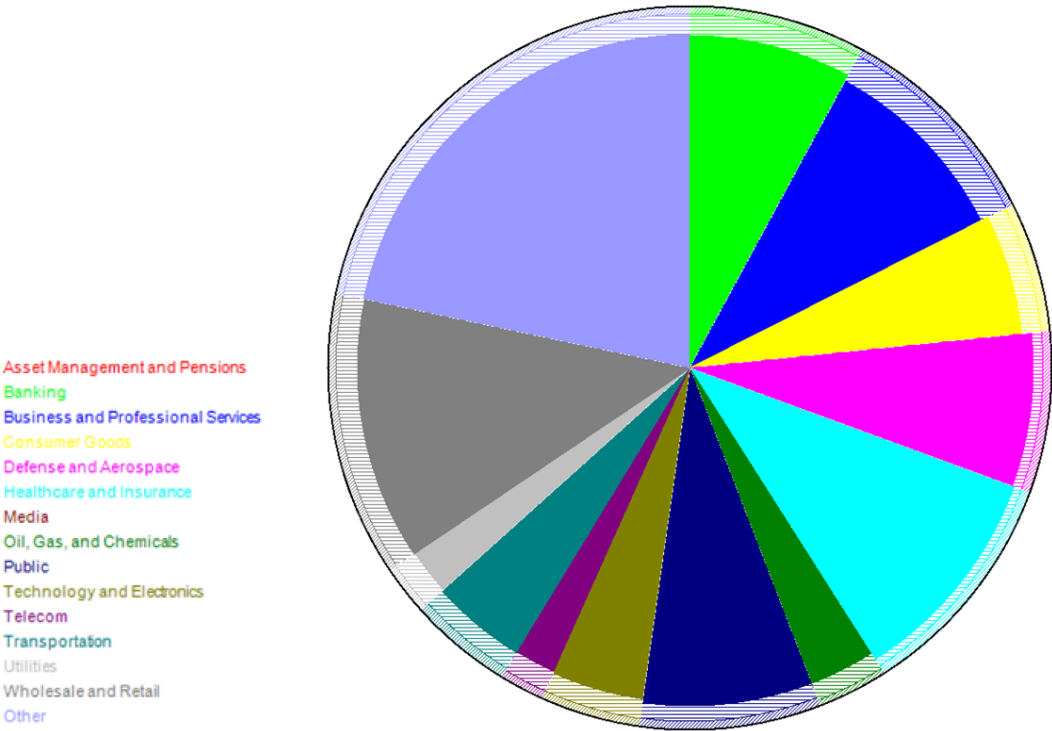


Figure 4.8. Cost of Cyber Crime in the Netherlands, Model 2: Breakout of Damages by Sector



NOTE: Horizontal shaded regions at outer edge denote systemic losses, and solid regions at center denote direct losses.

Figure 4.9. Cost of Cyber Crime in the Netherlands, Model 3: Distribution of Total GDP Costs

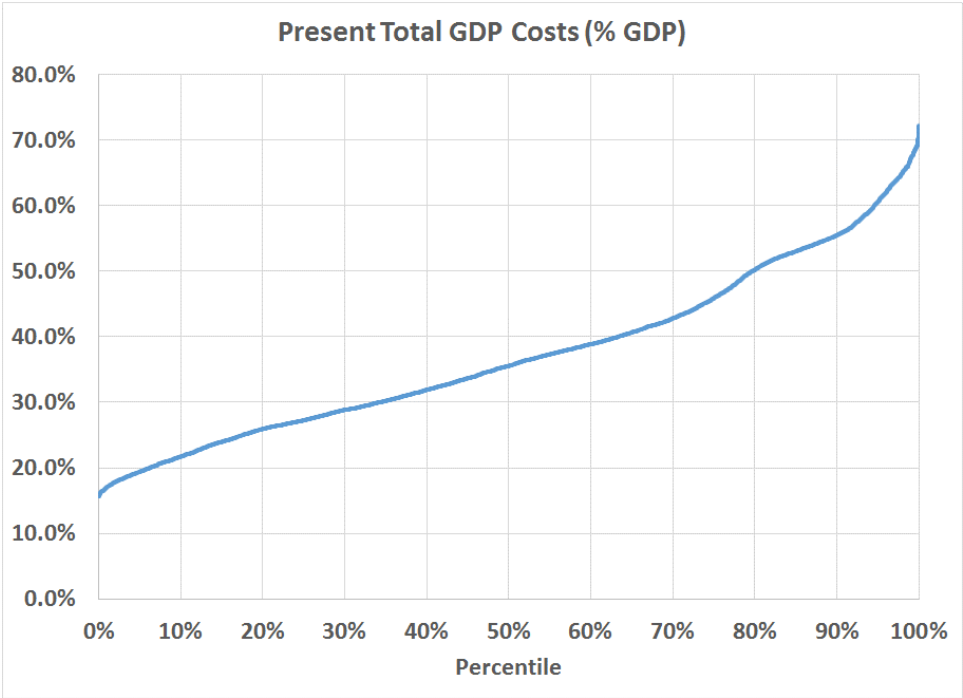
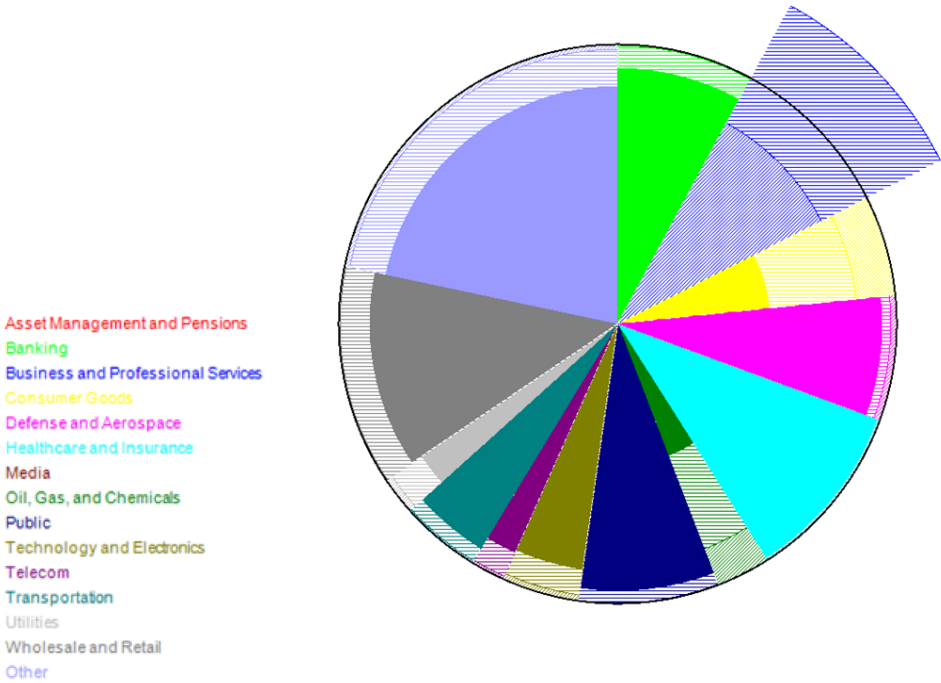


Figure 4.10. Cost of Cyber Crime in the Netherlands, Model 3: Breakout of Damages by Sector



NOTE: Horizontal shaded regions denote systemic losses, and solid regions denote direct losses.

Sample Case Study: Lloyd's Business Blackout

Several of the case studies mentioned previously focus on attacks against a particular industry—for example, recent DDoS attacks against financial services or an attack on the power grid. Although our model was not specifically designed for this purpose, it can be used to conduct a sector-specific analysis of either (1) direct costs or (2) direct plus systemic costs. In practice, it handles such scenarios by modeling the impacts on a single sector or subset of sectors and zeroing out all other effects. Notably, this can be done while still allowing for the associated propagation of systemic impacts to all industry sectors.

Although our model is focused on the period of a year for each run, the duration of many of these scenarios differs. Fortunately, it is relatively easy to scale our model to represent different time periods—assuming a linear time distribution of risk. This can be achieved by adjusting the severity and scale inputs to the desired period where $1 = 100\% = \text{loss of all output for one year}$. For example, if the attack resulted in loss of all output for one month and then a complete recovery for the subsequent 11 months, the value would be $1/12 = 0.083$. Similarly, different values for different time periods can also be represented by aggregation. In the previous example, if recovery was only 50 percent in the second month before full recovery in the third month, the value would be $0.083 + 0.042 = 0.125$.

To illustrate this discussion with a practical example, we walk through the use of our model to represent the scenario in the Lloyd's *Business Blackout* report.⁴² In this scenario, power goes out for one-third of the United States for approximately two weeks (all sectors in one-third of the United States go down entirely for two weeks), and utilities take about a year to recover (their IP and net income are entirely lost for the year).

In our model, we would use

- exposure-peril relationship (X_{cep}):
 - Set the exposure-peril relationship equal to $1/3 = 0.33$ for the three pairings of the peril of degradation, destruction, and corruption to all exposure types. Set the exposure-peril relationship equal to 0 percent for all other pairings.
- sector-exposure relationship (Y_{cie}):
 - Set the sector-exposure relationship equal to $2/52 = 0.038$ for the 15 pairings of the exposure of net income to all sector types.
 - Set the sector-exposure relationship equal to Module 1 for the two pairings of either the exposure of capital assets or of IP to the sector type of utilities. Set the sector-exposure relationship equal to 0 for the 28 remaining pairings.

Applying this calculation yields, on average, **direct losses in the United States of \$184 billion and total losses of \$515 billion**. Lloyd's study considered three scenarios that reported losses from \$243 billion to \$1.024 trillion.⁴³

⁴² Lloyd's, 2015.

⁴³ Lloyd's, 2015.

The first iteration of this model will create many opportunities for improvement, and, with regard to the discussion above, we wish to highlight at least two areas for additional work. The first is to address the assumption of linear distribution of economic impact in any given year. For scenarios with shorter durations, this will provide the modeler options for greater fidelity. The seasonality of GDP could be adjusted based on historical data to account for how the timing of an attack during periods of higher or lower economic activity (e.g., the holiday shopping season) might affect the results. The second improvement, which is perhaps the most important, would be to accurately model downstream systemic risk propagation. In the canonical examples of an attack against the cloud or the grid, this would allow our model to represent the impacts of an outage or disruption to users of those services. A potential stand-in or shortcut for this data-intensive task is to leverage previous studies on sensitivities by industry to particular inputs, such as information and communication technologies use or energy.

Sensitivity to the Choice of Probability Distribution Functions

Given the wealth of possible distributions in the model, as well as the difficulty in expressing extreme tail distributions, we conducted a sensitivity study of Model 3 (VaR) to the adoption of different distributions. Recall that Table 3.8 shows the 25th-, 50th-, 75th-, and 95th-percentile bootstrapped values of attack cost per revenue used to create the X_{cep} in Model 3. We attempted three different fits, as shown in Table 4.2:

- **Uniform distribution.** Here, we chose to model data ranging from the 25th to 75th percentile. Using defense and aerospace as a model sector, this results in $U(0.0023, 0.12)$.
- **Triangular distribution.** Here, we wanted to model the extreme tails as being present but less likely by skewing the mean of the data toward 0. There are many options that artificially cause this; here, we assume that the data are skewed toward the 25th percentile and bounded by the 75th percentile. Using defense and aerospace as a model sector, this results in $T(0.0023, 0.0023, 0.12)$.
- **Beta distribution.** Most of the data in the Advisen data set appear to provide a beta distribution. Using defense and aerospace as a model sector, this results in $B(0.06, 0.35)$.

Figure 4.11 shows the resulting probabilistic distribution of total costs for these three options. The beta distribution captures the presence of the extreme tails; their extent is highly dependent on the choice of beta parameters. The uniform and beta tend to agree between the 20th and 60th percentiles. The artificially imposed changes to the use of the triangular distribution cause those results to underestimate damages compared with the results using a beta distribution.

Recall that the data for Model 3 were taken from the Advisen data set, which is known to be only a small subset of the actual data. Because many of the percentiles were created with small numbers of events, it seems that trying to fit a distribution to the extreme tails would provide meaningless results. In addition, because the data set is weighted toward larger events (those that would need to be reported, as opposed to those that might have small damages and then go

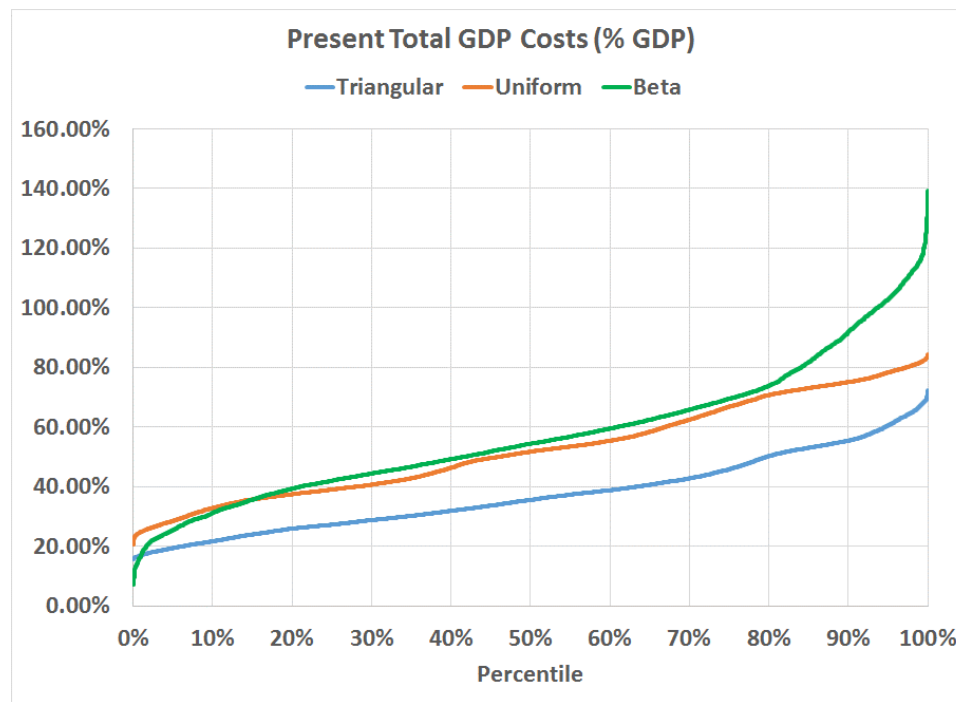
unreported), it seems that a triangular distribution with a higher weighting on less costly events might make sense. Hence, we use the triangular distributions in this chapter.

Table 4.2. Model 3: Capital Assets Sector Exposure Best Fits for Different Distributions

Sector Exposure	Uniform	Triangular	Beta
Asset management and pensions	U(0.0023,0.12)	T(0.0023,0.0023,0.12)	B(0.06, 0.35)
Banking	U(0.00017,0.031)	T(0.00017, 0.00017,0.031)	B(0.06, 0.35)
Business and professional services	U(0.012, 1.97)	T(0.012,0.012, 1.97)	B(0.12, 0.17)
Consumer goods	U(0.0017, 0.80)	T(0.0017,0.0017, 0.80)	B(0.12, 0.23)
Defense and aerospace	U(0.0023,0.12)	T(0.0023,0.0023, 0.12)	B(0.06, 0.35)
Health care and insurance	U(0.00032, 0.033)	T(0.00032,0.00032, 0.033)	B(0.06, 0.35)
Media	U(0.0023,0.12)	T(0.0023,0.0023,0.12)	B(0.06, 0.35)
Oil, gas, and chemicals	0.26	0.26	0.26
Public	U(0.000083, 0.0082)	T(0.000083,0.000083, 0.0082)	B(0.03, 1)
Technology and electronics	U(0.0023,0.12)	T(0.0023,0.0023,0.12)	B(0.06, 0.35)
Telecom	U(0.00013, 0.068)	T(0.00013, 0.00013, 0.068)	B(0.06, 0.35)
Transportation	U(0.000049, 0.047)	T(0.000049, 0.000049, 0.047)	B(0.06, 0.35)
Utilities	U(0.0014, 0.15)	T(0.0014,0.0014, 0.15)	U(0.0014, 0.15)
Wholesale and retail	U(0.000079, 0.035)	T(0.000079, 0.000079, 0.035)	B(0.08, 0.6)
Other	U(0.0023,0.12)	T(0.0023, 0.0023, 0.12)	B(0.06, 0.35)

NOTE: Some sectors had very few events reported and thus have even simpler distributions as best fits.

Figure 4.11. Cost of Cyber Crime in the Netherlands, Model 3: Breakout of Damages by Sector



Chapter 5: Conclusion and Next Steps

This report presents a transparent and adaptable methodology for estimating present and future global costs of cyber risk that acknowledges the considerable uncertainty in the frequencies and costs of cyber incidents. This methodology (1) identifies the value at risk by country and industry sector; (2) computes **direct costs** by considering multiple financial exposures for each industry sector and the fraction of each exposure that is potentially at risk to cyber incidents; and (3) computes the **systemic costs** of cyber risk between industry sectors using OECD input, output, and value-added data across sectors in more than 60 countries. To incorporate uncertainty into the model, we allowed many of the parameters to be defined by point estimates or probability distributions. In our model, we include uniform, triangular, trapezoidal, and generalized beta distributions, along with a Delphi distribution, where a set of values or distributions are equally likely to be chosen (often used in response to elicitation from multiple subject-matter experts). Outputs are either average values or cumulative distributions of these costs across countries and sectors. We emphasize that these sample sets are meant to illustrate potential uncertainties and related studies; to that end, we have attempted to call out caveats and uncertainties.

The “as-is” model affords the user the ability to extend any particular analysis from specific countries to a global scale, model impact on GDP in a range of sectors, and model actual events. Sample questions that could be addressed with this model include the following: What is the global cost of cyber crime? How much damage will a cyber-induced blackout incur? What are potential downstream costs? How will cyber controls affect costs?

Users will likely want to update model assumptions to investigate their research question of choice. The examples provided in the model were built with publicly available data, and there are a number of potential improvements to sets and inter-set relationships (e.g., peril exposure or sector exposure). For instance, a user could update the exposures calculation by examining multiple years of balance sheets and match IP in one year to revenue in the next. Or a user could theoretically express asset-related harms in income-statement terms by amortizing the asset damage over a set period of years, which would yield an annual amortization expense. In addition, a user could conduct an expert elicitation (e.g., Appendix F) to reduce uncertainty. Furthermore, a researcher could test country-specific factors, such as the level of technology advancement in the country; the general level of cybersecurity expertise in the same country; and related factors, such as levels of governance and stability in that jurisdiction. Data from such sources as the International Telecommunication Union and the World Bank could be leveraged in such an effort. If a user also had confidential information, they could also apply these to the model. Or if users dislike the exposures set, they could define and implement a different set of exposures and their relations to the other sets. These could be calculated by altering the data set

itself, the list of data members on the “Data Element Lists” worksheet, and the appropriate lookup table on the “Data Locations” worksheet in the Excel spreadsheet model.

Another topic is the current and future impact of cyber controls and defenses. For example, consider the difference between protection of data in a consumer-driven sector (e.g., banking and retail) compared with a sector related to national security (e.g., aerospace and defense); it is likely that these sectors will have different defenses. To capture this, a user could update the sector-exposure or peril-exposure table as needed to indicate that some of these previously targetable exposures are no longer targetable by particular perils. Alternatively, a user could insert an intermediate matrix in between the sector-exposure and exposure-peril tables calculation to account for defenses. This approach would also work if a user feels that particular sectors are more susceptible than others to a particular kind of attack.

In this study, systemic effects are limited to the upstream effect, and therefore one area of potential future research is inclusion of downstream systemic effects. For example, let us assume that there was an attack on the U.S. utilities sector. Our model first calculates the direct costs to the utilities sector in the United States, such as costs to replace damaged hardware and business interruption loss. This is a function of perils and exposures. Now, given that utilities are damaged, there is likely damage both upstream (companies that used to sell parts to the sector of utilities but cannot sell as many because the demand is reduced) and downstream (lights are out and other sectors cannot function). Our model calculates upstream but not downstream impacts. Yet, a user may be interested in downstream effects. The World Economic Forum has a white paper on understanding systemic cyber risk that describes how downstream systemic loss might propagate.⁴⁴ Likewise, it could be possible to model economic impacts of disruptive cyber events based on impacts of disruptive non-cyber events that would have had similar effects. One example would be the 2003 Northeast blackout for which economic impact has been estimated.⁴⁵ To include this in the model, a user would update the systemic cost input-output matrix multipliers with additions for the downstream fractions.

⁴⁴ World Economic Forum, 2016.

⁴⁵ Electricity Consumers Resource Council, 2004.

Appendix A: Estimating the Global Cost of Cyber Risk Calculator User Manual

The Estimating the Global Cost of Cyber Risk Calculator (which, for simplicity, will be referred to as *the calculator* for the remainder of this appendix) implements the methodology described in this document. It is a Microsoft Excel–based tool paired with a small Windows executable file to generate pie charts (as shown in Figure 4.10, for example). The tool has been tested on versions of Microsoft Excel 2011 and in Windows. It has not been tested on Mac Excel, but the pie-chart generator is disabled on machines running Mac OS. All the calculations in the tool are done using Visual Basic, so macros must be enabled for the calculator to work.

When the calculator opens, it begins on the *Start Page*⁴⁶ worksheet. The *Start Page* contains the contact information for the author and instructions for navigating through the worksheets and entering data. The tabs for the different classes of worksheet are denoted with different colors. The *Start Page* and *License Agreement* are denoted by blue tabs, input sheets are denoted by green tabs, output sheets are denoted by purple tabs, and the OECD data sheets are denoted by red tabs. Note that the structure of these OECD sheets should not be adjusted because the tool assumes a very particular structure to these sheets, although updated data could populate them if available. Instructions are in orange boxes at the top of each worksheet, and values to be entered by the user are in yellow cells.

Input Sheets (Green Tabs)

Data Element Lists

There are five sets of elements used in our models: the GDP categories from the OECD data, the countries of interest, the industry sectors, the cyber perils faced, and the economic exposures to cyber perils. If a user modifies any of these elements, new table templates will need to be created using the **Generate Table Templates** and **Generate Sector-Category Map** buttons. These buttons will generate new tables for the user to fill on the *Peril-Exposure Template*, *Sector-Exposure Template*, and *Sector-Category Map* worksheets, removing all data from the sheets while doing so. The user should not modify the GDP categories elements, as they reference the OECD data worksheets for each country.

⁴⁶ Worksheet names are presented *in italics*. Button labels are in **bold**.

Data Locations

For each country, the user specifies five worksheets to define the necessary parameters for the cost calculations: the OECD data worksheet (for GDP and input-output values by GDP category) and present and future Peril-Exposure and Sector-Exposure worksheets. The country names listed on this sheet in the first column will also appear in the drop-down menus on the output sheets. OECD data were available from 2011 for 62 countries regarding GDP and input-output production data by category. A user wanting to add a new country to the tool that does not have OECD data available should pick a similar country that does have OECD data available and use its values by proxy to generate the necessary GDP and Leontief inverse matrixes. The method for properly scaling the GDP of the new country is described in the *GDP Map 2011–2016* section below.

Sector-Category Map

This worksheet associates each GDP category on the OECD worksheets to an industry sector used in the model. Each OECD GDP category should be mapped to one of the industry sectors in the model by entering an X in the appropriate row.

GDP Map 2011–2016

This worksheet gives the GDP change by industry sector from 2011 to 2016 for each country and is used to map the 2011 OECD data to 2016. If a country name does not appear on this worksheet, it is assumed that there has been no GDP change from 2011 to 2016 in all sectors. If a new country (A) is added to the tool and the OECD data of country B are used by proxy, to represent the correct GDP for country A into the model, if G_A and G_B are the 2016 GDPs of the respective countries, and then if $g_{B,i}$ is the growth in industry sector i in country B from 2011 to 2016, then $g_{A,i} = g_{B,i} (1 + G_A/G_B)$ will correctly map the growth in country A that will produce the desired GDP for country A.

GDP Map Future

For each country and industry sector, this worksheet gives the projected future annual GDP change. It is used to map the values calculated for 2016 to a future year specified on the *Data Element Lists* worksheet. If a country name does not appear on this worksheet, it is assumed that there will be no annual GDP change in all sectors. Only point estimates of annual growth can be entered in this table, not distributions. There is no need for a country using proxy OECD data to match that country's future GDP predictions.

Peril-Exposure Template and Sector-Exposure Template

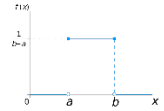
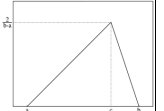
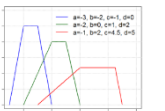
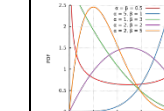
When the **Generate Table Templates** button on the *Data Element Lists* sheet is clicked, it updates both worksheets listed above. The intent is that the user would then make copies of these

worksheets as needed and populate them with point estimates and/or probability distributions for analysis. The names of these new worksheets would then be added to the *Data Locations* sheet. The *Sector-Exposure Template* sheet contains the table structure to enter the amount of each sector output that is at risk for each exposure. The *Peril-Exposure Template* sheet contains the table structure in which to enter the effect of each peril on each financial exposure in each industry sector (as a percentage of the financial exposure). For the *Peril-Exposure* worksheet, the default values are assumed to apply across all sectors, but values may be entered for specific industry sectors. Entries in these worksheets may be point estimates (a number) or a probability distribution. Allowable distributions are

- $U(a,b)$: uniform random variable between a and b
- $B(\alpha, \beta, [\min, \max])$: beta distribution with parameters α and β and optional range \min [0] to \max [1], with 0 and 1 used as the default values if not included, respectively
- $T(a,b,c)$: triangular distribution with minimum a , mode b , and maximum c
- $Q(a,b,c,d)$: trapezoidal distribution with minimum a , mode between b and c , and maximum d
- $D(\text{dist1}|\text{dist2}|\dots)$: Delphi distribution, where each entry in the pipe-separated list is equally likely to be chosen. Entries may be numbers or distributions, such as $D(0.4|0.6)$ or $D(T(0,0.5,1)|T(0.3,0.6,0.9))$.

Table A.1 shows the shape of the distribution function for each case and provides the expected value for each distribution. The calculator will quit if the values in these tables are not point estimates or one of the probability distributions above. The tables used to generate the results in this report are included as examples in the tool.

Table A.1. Probability Distributions Allowed in Calculator

Distribution	Point Estimate	Uniform Distribution	Triangular Distribution	Trapezoidal Distribution	Generalized Beta Distribution	Delphi Distribution
Notation in calculator	Single number, q	$U(a,b)$	$T(a,b,c)$	$Q(a,b,c,d)$	$B(\alpha, \beta, [\min, \max])$	$D(\text{dist}_1 \text{dist}_2 \dots \text{dist}_n)$
Expected value ($E[X]$)	q	$(a+b) / 2$	$(a+b+c) / 3$	$((d^2 + cd + c^2) - (a^2 + ab + b^2)) / (3 * (a + b - c - d))$	$\min + (\max - \min) * (\alpha / (\alpha + \beta))$	$(E[\text{dist}_1] + \dots + E[\text{dist}_n]) / n$
Probability distribution function	N/A					N/A

Output Sheets (Purple Tabs)

Three kinds of output, one each on a sheet, are generated.

Outputs

This sheet displays a number of output tables for each country:

- Present/Future Input-Output Matrix (% of Sector Output)
- Present/Future Input-Output Matrix (\$M)
- Present/Future Inverse Leontief Matrix
- Present/Future Direct EV + Systemic EV Costs + GDP (by Sector).

The first three types of tables display intermediate calculations in the GDP and systemic costs estimation. If the GDP by sector table is selected, a pie chart displaying GDP, direct costs, and systemic costs (in diagonal and horizontal hatching, respectively) for each sector is shown. The columns on the table are color coded (and hatched) identically to the segments of the pie. Note that the *piemaker.exe* executable file must be in the same directory as the Excel worksheet for the pie chart to be generated, and the pie charts will not be generated on a Mac.

*RDM Outputs*⁴⁷

RDM is short for Robust Decision Making; the *RDM Outputs* sheet attempts to show the variability of the results due to the probability distributions that populate the *Peril-Exposure* and *Sector-Exposure* sheets. This sheet estimates for the specified country the cumulative distribution of costs via multiple random draws of each distribution in the *Peril-Exposure* and *Sector-Exposure* sheets. In addition to a table showing the result of each set of random draws, the worksheet contains a chart that shows the estimate of the cumulative distribution function for either the present or future direct, systemic, and total costs, either in dollars or as a percentage of GDP.

Global Outputs

This table displays for all countries a sector-by-sector breakdown of present or future direct, systemic, or total costs, either in dollars or as a percentage of GDP. The total across all countries in the model is also given in the last row of the table.

OECD Sheets (Red Tabs)

The structure of these sheets should not be modified unless the user identifies new data to update the sheets.

⁴⁷ See <https://www.rand.org/topics/robust-decision-making.html> for more information about RDM.

Appendix B: Review of Model Assumptions

Scope

This model assumes that an attack affects one and only one country at a time. Thus, we assume that a given target (and its exposed components) can be resolved into country-level elements. An attack with direct impacts in multiple countries would be handled by running the model across those elements in the affected countries. We can only calculate losses for countries and sectors listed in our model.

We have identified all sectors that can be directly affected by cyber attack; other sectors can have no direct losses but may have systemic losses. We can calculate economic losses within a sector (direct and indirect) rolled together in one. We can calculate some kinds of systemic losses (e.g., upstream but not downstream).

Note that this model does not calculate international network effects (the macroeconomic impacts experienced by other countries' sectors due to direct damages). While of significant research interest to RAND, this extra layer is not possible to create, given current techniques.

Impacts of Controls, Insurance, or Other Mitigation Methods

The guidance from our sponsors and the advisory committee directed us away from specifically including cybersecurity controls, insurance, or other mitigation methods in this model. Accordingly, the model can be updated to include them but does not focus on them. To include controls or insurance, a user could alter the sector-exposure relation. Insurance can also be thought of as simply a transfer from one agent to another to cover costs. These transfers would be a net benefit if they allowed a firm to reduce business interruptions or downtime, but, generally, business interruption insurance reimburses firms after an event has taken place and after the event has been contained.

Assumption That Changes in Growth of GDP Scale with Changes in Revenue

The Y_{cie} modules presented assume that the relationship between output (revenue) and value added (GDP) are fixed across time and that the composition of the economy of any country is also fixed across time. This implies that the intermediate inputs needed to produce goods in a specific sector are also fixed but does not imply that the capital-to-labor ratio is fixed, as we do not distinguish between payments to capital versus payments to labor. These two assumptions taken together allow us to assume an exogenous GDP growth rate and allocate the growth to each sector in a manner that is consistent with aggregate growth. Although it would be preferable to have sector-specific growth rates, it is difficult to reconcile sectoral growth with aggregate

growth. We distinguish growth rates based on the current income classifications by the World Bank to allow for cross-country differences that we know exist.

Appendix C: Module Y2 Sector-Exposure Relationship

Financial data from 4,447 publicly traded firms for 2013 through 2016 were collected to estimate the regression. As described earlier, recall that this regression estimates changes on firm revenue as a function of changes in R&D spending (a proxy for IP), net income, and total assets by sector as follows:

$$\log(\text{Revenue}_i) = \beta_1 \log(\text{R\&D}_i) + \beta_2 \log(\text{NetIncome}_i) + \beta_3 \log(\text{TotalAssets}_i) + \epsilon \quad \forall i \in I.$$

Tables C.1 to C.3 display the full results, significance, and fit of each regression.

Table C.1. Results of Sector-Exposure Regressions: R&D

Sector	n	R ²	Coeff.	R&D		
				Std Er.	t	P> t
All sectors	2,958	0.99	0.02	0.01	2.17	0.03
Banking	28	0.99	0.06	0.12	0.45	0.65
Business and professional services	137	0.99	0.16	0.06	2.80	0.01
Consumer goods	1,012	1.00	-0.06	0.01	-4.64	0.00
Health care and insurance	-	-	-	-	-	-
Oil, gas, and chemicals	141	1.00	0.17	0.03	6.78	0.00
Public	15	1.00	-0.12	0.10	-1.28	0.22
Technology and electronics	194	0.99	0.00	0.04	0.12	0.91
Telecom	299	0.99	0.14	0.04	4.03	0.00
Transportation	12	1.00	-0.19	0.06	-3.24	0.01
Utilities	9	0.99	0.66	0.31	2.12	0.08
Other	1,035	1.00	-0.03	0.01	-3.13	0.00

NOTE: Some sectors are not included due to insufficient data.

Table C.2. Results of Sector-Exposure Regressions: Net Income

Sector	n	R ²	Coeff.	Net Income		
				Std Er.	t	P> t
All sectors	2,958	0.99	0.04	0.01	4.26	0.00
Banking	28	0.99	-0.04	0.11	-0.34	0.73
Business and professional services	137	0.99	0.02	0.05	0.44	0.66
Consumer goods	1,012	1.00	0.05	0.01	4.10	0.00
Health care and insurance	-	-	-	-	-	-
Oil, gas, and chemicals	141	1.00	0.16	0.05	3.62	0.00
Public	15	1.00	0.15	0.09	1.61	0.13
Technology and electronics	194	0.99	0.02	0.03	0.54	0.59
Telecom	299	0.99	-0.05	0.03	-1.80	0.07
Transportation	12	1.00	-0.02	0.16	-0.16	0.88
Utilities	9	0.99	0.11	0.45	0.24	0.82
Other	1,035	1.00	0.07	0.01	5.14	0.00

NOTE: Some sectors are not included due to insufficient data.

Table C.3. Results of Sector-Exposure Regressions: Total Assets

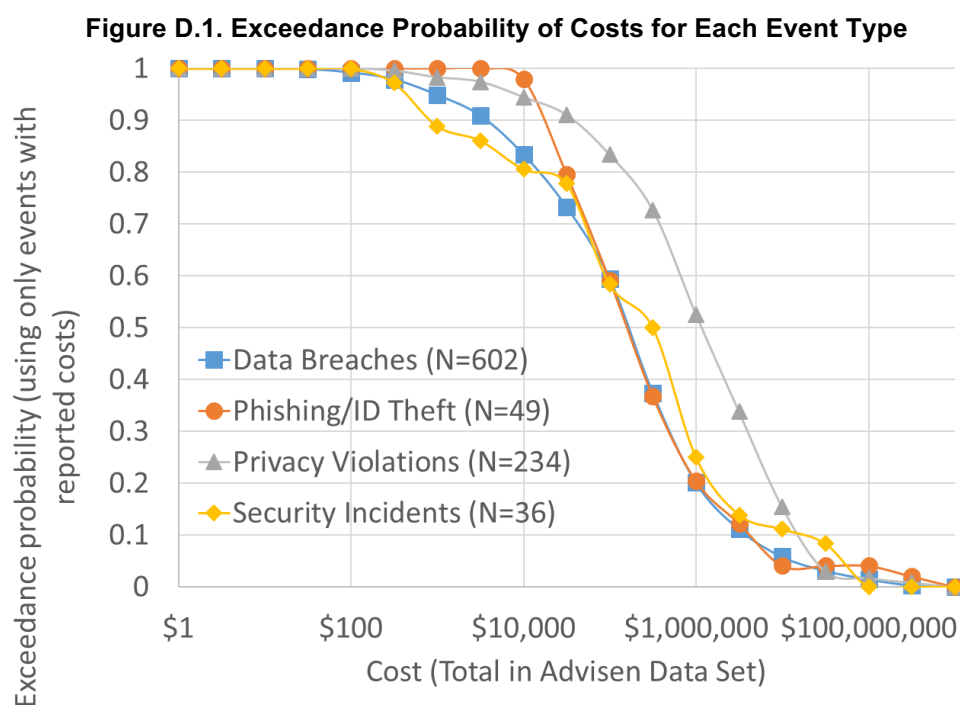
Sector	<i>n</i>	<i>R</i>²	Coeff.	Total Assets	
				Std Er.	<i>t</i>
All sectors	2,958	0.99	0.01	164.80	0.00
Banking	28	0.99	0.06	14.07	0.00
Business and professional services	137	0.99	0.04	21.85	0.00
Consumer goods	1,012	1.00	0.01	112.83	0.00
Health care and insurance	-	-	-	-	-
Oil, gas, and chemicals	141	1.00	0.03	26.70	0.00
Public	15	1.00	0.05	18.98	0.00
Technology and electronics	194	0.99	0.02	39.61	0.00
Telecom	299	0.99	0.02	38.62	0.00
Transportation	12	1.00	0.08	13.16	0.00
Utilities	9	0.99	0.33	1.87	0.11
Other	1,035	1.00	0.01	109.99	0.00

NOTE: Some sectors are not included due to insufficient data.

Appendix D: Advisen Data

The Advisen data set⁴⁸ contains more than 12,000 incidents classified into five separate entries for event type and 11 separate entries for case type. Table 3.1 maps each case type to its most likely event type. Note that some cyber events would not be covered by the case types listed here (e.g., cyber warfare). Other events that might have difficulties fitting into this taxonomy are the Sony Pictures hack, the Democratic National Committee hack, the Ukraine electric infrastructure outage, and a government hacking a technology company and then producing similar technology six months later.

Of the more than 12,000 incidents, only about 930 contain data on costs. Costs are provided in several categories (response, estimated, award, settled, first, third, and total). Exceedance-probability curves for cost for the non-null event types are given in Figure D.1. In this data set, the privacy violations ($N = 234$) are more expensive than other events; data breaches ($N = 602$), phishing and identify theft ($N = 49$), and security incidents ($N = 32$) have similar exceedance probability curves. Note that the horizontal axis is logarithmic; on a regular graph, there is a greater difference between event types.



NOTES: The horizontal axis is a logarithmic scale. Exceedance probabilities are a function only of the incidents where cost was reported. We could not identify the difference between an incident with zero cost and an incident with an unreported cost, so all incidents without a cost listed are omitted.

⁴⁸ See Advisen (2017) for more information about the data set.

Appendix E: Characterizing Attackers and Perils

This appendix provides a taxonomy for characterizing attackers and perils. Potential attackers are categorized by their overarching goal. Attacker methods are loosely described, but they are not absolute. The probability of a given activity and level of severity varies. Highly capable attackers can also engage in less difficult actions; simpler attacks should be considered lesser-included cases of the attacks described below and listed in Table E.1.

Individuals may engage in attacks, defacement, exploration, or seeking some form of personal gain. Perhaps surprisingly, the probability of individuals doing this is very high, but the level of damage they cause is generally quite low. For example, students attempting to improve their permanent records, transit riders interested in getting an unlimited free bus pass, or curious individuals who just want to know how systems fit together might all engage in exploration and then take advantage of whatever they find.

Table E.1. Attacker and Threat Characterizations

Who	How: High-End Threat (Lesser-included cases are also considered)	Example
Individuals	Attack, deface, or explore systems for curiosity, fun, personal gain, or anomie	Students changing grades, riders adjusting status of bus passes
Petty criminals	Attack systems, databases, or users or collect information for profit	Sextortion, wire fraud
Terrorists	Attack systems, databases, or users from a target to damage them, or deface them to engage in a propaganda campaign	Defacement of news sites, DDoS attacks against political target
Hactivists	Attack or deface a system for propaganda purposes	Defacement of news sites, DDoS attacks against political target
Corporate spies	Gather intelligence about a competitor's activities	Gaining access to a competitor's list of clients, blueprints, or proprietary research
Government spies	Gather intelligence about an adversary's activities	Access to an adversary's internal communications
Organized crime	Exploit or attack systems, databases, or users for profit; gather intelligence about government or adversary activities	Access to law enforcement communications for intel purposes, rentable botnets for profit purposes
Military (or military-like) cyber unit	Degrade, disrupt, or destroy an adversary's capabilities via cyber capabilities	DDoS attacks on adversary government websites, disruption of internal government communications
Cyber-enabled kinetic unit	Degrade, disrupt, or destroy an adversary's capabilities via kinetic capabilities compounded by cyber capabilities	Degradation of adversary communications in conjunction with electronic warfare, disruption of adversary civilian Incident Command System-managed systems leading to physical effects
Insider threat	Disrupt operations, sell intelligence, deface or distribute intelligence for propaganda purposes	Remotely resetting former employer's passcodes, leak of proprietary information

Appendix F: Potential Expert Elicitation Format

We developed an expert elicitation framework to define the exposure-peril relationship (Tables F.1 and F.2). The associated expert elicitation tool allows experts to indicate approximate, relative levels of risk in three scenarios of risk level. Doing so does not indicate the level of loss; rather, it indicates experts' perceptions of relative levels of value at risk by sector and potential threat. Pain is independent of sector and can be considered as a percentage of assets, IP, and income. Information about sector percentage of GDP and exposure rate is set. 0 is no pain, and 100 is catastrophic. In the case of the sector vulnerability, experts are invited to approximate the relative vulnerability of sectors. While information and communications technology or energy dependence may be used as approximations of the relative vulnerability of a sector, this expert elicitation invites qualitative judgment to be expressed. When several experts provide their input, the data can then be used to create a triangle of probability for random draws of inputs.

Table F.1. Pain-Level Elicitation Worksheet

Peril	Target	Pain Level of Best-Case Scenario (0–100%)	Most Likely Pain Level (0–100%; must be equal to or between best-case and worst-case pain levels)	Pain Level of Worst-Case Scenario (0–100%)
Exfiltration of company data	IP			
Exfiltration of customer data	IP			
Degradation, destruction, and corruption	IP			
Disruption of business and denial of service	IP			
Exfiltration of company data	Capital assets			
Exfiltration of customer data	Capital assets			
Degradation, destruction, and corruption	Capital assets			
Disruption of business and denial of service	Capital assets			
Exfiltration of company data	Net income			
Exfiltration of customer data	Net income			
Degradation, destruction, and corruption	Net income			
Disruption of business and denial of service	Net income			

Table F.2. Sector Variation Elicitation Worksheet

Sector	Vulnerability of This Sector	What Sector Have You Chosen for the Generic Sector?
Generic sector	1.00	
Sector	Vulnerability of this sector compared with generic sector (e.g., 0.25 means a quarter as vulnerable, 2 means twice as vulnerable)	Further notes and explanations
Asset management and pensions		
Banking		
Business and professional services		
Consumer goods		
Defense and aerospace		
Health care and insurance		
Media		
Oil, gas, and chemicals		
Public		
Technology and electronics		
Telecom		
Transportation		
Utilities		
Wholesale and retail		
Other		

References

- Advisen, *Liability of Technology Companies for Data Breaches*, 2010.
- Advisen, “Cyber Loss Dataset,” 2017. As of January 2, 2018:
<https://www.advisenltd.com/data/cyber-loss-data/>
- Association for Financial Professionals, *2015 AFP Payments Fraud and Control Survey: Report of Survey Results*, 2015.
- Bodeau, D., R. Graubart, and J. F. Greene, “Improving Cyber Security and Mission Assurance via Cyber Preparedness (Cyber Prep) Levels,” MITRE Corporation, 2009. As of January 4, 2018:
https://www.mitre.org/sites/default/files/pdf/09_4656.pdf
- Conti, G., T. Cross, and D. Raymond, “Pen Testing a City,” *Black Hat*, 2015. As of January 4, 2018:
<https://www.blackhat.com/docs/us-15/materials/us-15-Conti-Pen-Testing-A-City-wp.pdf>
- Davis, J. S., B. A. Boudreaux, J. W. Welburn, J. Aguirre, C. Ogletree, G. McGovern, and M. Chase, *Stateless Attribution: Toward International Accountability in Cyberspace*, Santa Monica, Calif.: RAND Corporation, RR-2081-MS, 2017. As of January 4, 2018:
https://www.rand.org/pubs/research_reports/RR2081.html
- Deloitte, *Cyber Value at Risk in the Netherlands*, 2016. As of January 4, 2018:
<https://www.thehaguesecuritydelta.com/images/deloitte-nl-risk-cyber-value-at-Risk-in-the-Netherlands.pdf>
- Dreyer, P., *Estimating the Global Cost of Cyber Risk Calculator*, Santa Monica, Calif.: RAND Corporation, TL-281-WFHF, 2018. As of January 4, 2018:
<https://www.rand.org/pubs/tools/TL281.html>
- Electricity Consumers Resource Council, “The Economic Impacts of the August 2003 Blackout,” February 9, 2004. As of January 4, 2018:
<https://elcon.org/wp-content/uploads/Economic20Impacts20of20August20200320Blackout1.pdf>
- Federal Bureau of Investigation, *2016 Internet Crime Report*, 2016.
- Gagnaire, M., F. Diaz, C. Coti, C. Cerin, K. Shiozaki, Y. Xu, P. Delort, J.-P. Smets, J. Le Lous, S. Lubiarz, and P. Leclerc, “Downtime Statistics of Current Cloud Solutions,” 2012. As of January 4, 2018:
<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.601.1031&rep=rep1&type=pdf>
- Gandel, S., “Lloyd’s CEO: Cyber Attacks Cost Companies \$400 Billion Every Year,” *Fortune*, January 23, 2015.
- Hiscox, *The Hiscox Cyber Readiness Report 2017*, 2017. As of January 4, 2018:
<https://www.hiscox.com/cyber-readiness-report>
- Jacobs, V., J. Bulters, and M. van Wieren, “Modeling the Impact of Cyber Risk for Major Dutch Organizations,” Deloitte Cyber Risk Services, *European Conference on Cyber Warfare and Security*, July 2016, pp. 145–154.
- Juniper Research, *The Future of Cybercrime & Security: Financial and Corporate Threats & Mitigation*, 2015.
- Kaspersky Lab, “Damage Control: The Cost of Security Breaches,” 2015. As of January 4, 2018:
<https://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf>

Lloyd's, *Business Blackout: The Insurance Implications of a Cyber Attack on the US Power Grid*, 2015. As of January 4, 2018:
<https://www.lloyds.com/~media/files/news-and-insight/risk-insight/2015/business-blackout/business-blackout20150708.pdf>

Lloyd's, *Counting the Cost: Cyber Exposure Decoded*, 2017. As of January 4, 2018:
<https://www.lloyds.com/news-and-insight/risk-insight/library/technology/countingthecost>

Lockheed Martin, "The Cyber Kill Chain," 2014. As of January 4, 2018:
<https://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html>

McAfee and the Center for Strategic and International Studies, *Net Losses: Estimating the Global Cost of Cybercrime*, June 2014. As of January 4, 2018:
https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf

National Institute of Standards and Technology, *Standards for Security Categorization of Federal Information and Information Systems*, FIPS 199, 2004. As of January 4, 2018:
<http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf>

National Institute of Standards and Technology, *Guide for Conducting Risk Assessments*, SP 800-30 Rev. 1, 2012. As of January 4, 2018:
<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>

NetDiligence, *Cyber Claims Study*, 2016. As of January 4, 2018:
https://netdiligence.com/wp-content/uploads/2016/10/P02_NetDiligence-2016-Cyber-Claims-Study-ONLINE.pdf

NIST—See National Institute of Standards and Technology.

OECD, "STAN Industry List," undated. As of January 4, 2018:
http://www.oecd.org/sti/ind/STANi4_Industries_ENG.pdf

OECD, "About the OECD," 2017a. As of January 4, 2018:
<http://www.oecd.org/about/>

OECD, "Brazil—Economic Forecast Summary (November 2017)," 2017b. As of January 4, 2018:
<http://www.oecd.org/brazil/brazil-economic-forecast-summary.htm>

OECD, "Input-Output Tables," 2017c. As of January 4, 2018:
<http://stats.oecd.org/Index.aspx?DataSetCode=IOTS>

OECD, "STAN STructural ANalysis Database," 2017d. As of January 4, 2018:
<http://www.oecd.org/sti/ind/stanstructuralanalysisdatabase.htm>

Ponemon Institute, *2012 Cost of Cyber Crime Study: United States*, 2012.

Ponemon Institute, *2013 Cost of Data Breach Study: Global Analysis*, 2013a.

Ponemon Institute, *Cost of Data Center Outages*, 2013b. As of January 4, 2018:
<https://www.ponemon.org/local/upload/file/2013%20Cost%20of%20Data%20Center%20Outages%20FINAL%202012.pdf>

Ponemon Institute, *2014 Cost of Data Breach Study: Global Analysis*, 2014.

Ponemon Institute, *2015 Cost of Data Breach Study: United States*, 2015.

Ponemon Institute, *2016 Cost of Data Breach Study: Global Analysis*, 2016.

Ponemon Institute, *2017 Cost of Data Breach Study: Impact of Business Continuity Management*, IBM, 2017. As of January 4, 2018:
<https://www.ibm.com/security/data-breach/>

- Rose, A., and D. Wei, “Estimating the Economic Consequences of a Port Shutdown: The Special Role of Resilience,” *Economic Systems Research*, Vol. 25, No. 2, 2013, pp. 212–232.
- Symantec, *An ISTR Special Report: Ransomware and Business 2016*, 2016. As of January 4, 2018:
https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ISTR2016_Ransomware_and_Businesses.pdf
- Thompson, I., “NotPetya Ransomware Attack Cost Us \$300m—Shipping Giant Maersk IT Crippled So Badly Firm Relied on WhatsApp,” *The Register*, August 16, 2017. As of January 4, 2018:
https://www.theregister.co.uk/2017/08/16/notpetya_ransomware_attack_cost_us_300m_says_shipping_giant_maersk/
- Wing, I. S., A. Z. Rose, D. Wei, and A. Wein, “Impacts of the USGS ARkStorm Scenario on the California Economy,” *Natural Hazards Review*, Vol. 17, No. 4, 2016.
- World Bank, “New Country Classifications by Income Level,” 2016. As of January 4, 2018:
<https://blogs.worldbank.org/opendata/new-country-classifications-2016>
- World Economic Forum, “Understanding Systemic Cyber Risk,” white paper, October 2016. As of January 4, 2018:
http://www3.weforum.org/docs/White_Paper_GAC_Cyber_Resilience_VERSION_2.pdf