SOLVING CYBER RISK

PROTECTING YOUR COMPANY AND SOCIETY

ANDREW COBURN • ÉIREANN LEVERETT • GORDON WOO

WILEY

Solving Cyber Risk

Founded in 1807, John Wiley & Sons is the oldest independent publishing company in the United States. With offices in North America, Europe, Australia, and Asia, Wiley is globally committed to developing and marketing print and electronic products and services for our customers' professional and personal knowledge and understanding.

The Wiley Finance series contains books written specifically for finance and investment professionals as well as sophisticated individual investors and their financial advisors. Book topics range from portfolio management to e-commerce, risk management, financial engineering, valuation and financial instrument analysis, as well as much more.

For a list of available titles, visit our website at www.wileyfinance.com.

Solving Cyber Risk

Protecting your company and society

ANDREW COBURN
ÉIREANN LEVERETT
GORDON WOO

WILEY

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.

Published simultaneously in Canada.

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services or for technical support, please contact our Customer Care Department within the United States at (800) 762-2974, outside the United States at (317) 572-3993, or fax (317) 572-4002.

Wiley publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at http://booksupport.wiley.com. For more information about Wiley products, visit www.wiley.com.

Library of Congress Cataloging-in-Publication Data

Names: Coburn, Andrew (Andrew W.), author. | Leverett, Eireann, author.
| Woo, G., author.
Title: Solving cyber risk: protecting your company and society / Andrew
Coburn, Eireann Leverett, Gordon Woo.
Description: Hoboken, New Jersey: John Wiley & Sons, Inc., [2019] | Series:
Wiley finance series | Includes bibliographical references and index. |
Identifiers: LCCN 2018035611 (print) | LCCN 2018037247 (ebook) | ISBN
9781119490913 (Adobe PDF) | ISBN 9781119490920 (ePub) | ISBN 9781119490937
(hardcover) | ISBN 9781119490913 (ePDF)
Subjects: LCSH: Computer security. | Data protection.
Classification: LCC QA76.9.A25 (ebook) | LCC QA76.9.A25 C577 2019 (print) |
DDC 005.8—dc23
LC record available at https://lccn.loc.gov/2018035611

Cover Design: Wiley
Cover Image: © iStock.com/scyther5

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Contents

About the Authors

The three authors worked together on the development of the leading cyber risk analysis model being used by the insurance industry today, and in the development of scenarios for regulating cyber risk. They are each specialists in different fields of risk and cyber technology.

ANDREW COBURN

Andrew is a specialist in risk, and is the architect of the Cyber Solutions risk model marketed by Risk Management Solutions, Inc. (RMS), the leading cyber risk model being used in the insurance industry today. He is a senior vice president of RMS and one of the main contributors to the creation of commercial catastrophe risk models over the past 25 years. His previous books include *Earthquake Protection* (John Wiley & Sons). He is also a Director of the Cambridge Centre for Risk Studies (CCRS), based in the business school of the University of Cambridge, where he has coordinated the cyber risk research program and been the lead author on a number of CCRS cyber risk publications, which have been highly cited. Cyber risk scenarios developed at the CCRS have been adopted as stress tests by industry regulators. He is a frequent speaker at conferences on risk and financial services.

ÉIREANN LEVERETT

Éireann is an ethical hacker with many years of experience in cyber security and the impacts of computer security failures and accidents. He is the founder of Concinnity Risks Ltd and a Senior Researcher on Cyber Risk at the Cambridge Centre for Risk Studies (CCRS) at the University of Cambridge. He has experience of compromising the security of organizations, and assisting them to improve their security postures through a variety of short- and long-term methods. While his background is in artificial intelligence (AI) and computer security, he has increasingly taken an interest in a risk-centric view of computer security, and how markets can help or hinder progress in defending the internet. He is a member of the Forum of Incident Response and Security Teams (FIRST; https://www.first.org), and regularly speaks at incident response and hacker conferences.

GORDON WOO

Gordon is a catastrophist with Risk Management Solutions, Inc. (RMS), focusing mainly on complex man-made insurance risks such as terrorism and cyber risk. Profiled in *Newsweek* magazine, he was described as one of the world's leading catastrophists. He has 30 years of experience in catastrophe risk consultancy, advising financial institutions, governments, and major corporations. He was educated at Cambridge University, with degrees in mathematics, theoretical physics, and computer science. He is a visiting professor at University College London, and an adjunct professor at Nanyang Technological University, Singapore. He is the author of the books *The Mathematics of Natural Catastrophes* and *Calculating Catastrophe*, published by Imperial College Press.

Acknowledgments

The authors are fortunate to be supported by some great teams who have helped them carry out much of the work presented in this book. We have tried to acknowledge individual contributions wherever possible, but we would like to acknowledge specifically the inputs of:

Cambridge Centre for Risk Studies

We have had the support of some of the best and brightest at the Cambridge Centre for Risk Studies, a world-leading research center at Judge Business School, University of Cambridge. We are particularly grateful to the Executive Directors: Simon Ruffle, Professor Danny Ralph, and Dr Michelle Tuveson, and to the cyber risk research team: Dr Jennifer Daffron at stroke, Jennifer Copic, Tamara Evan, Kayla Strong, Andrew Smith (Drew to his risk colleagues), Kelly Quantrill, James Bourdeau, Tim Douglas, and Dr Andy Skelton. We are particularly indebted to Olivia Majumdar for her help in getting this book under way.

We are also indebted to the companies that have sponsored the research into cyber risk at the Cambridge Centre for Risk Studies, including Lockheed Martin, Lloyd's of London (with particular thanks to Trevor Maynard for his support and encouragement), AXA XL, Pool Re, Citigroup, American International Group (AIG), Risk Management Solutions, Inc. (RMS), and all the other supporters that have included cyber risk within the range of multi-threat risk research.

Risk Management Solutions, Inc.

We very much appreciate the support of our colleagues at RMS in the cyber model development team, particularly the business leadership of Dr Mohsen Rahnama, Peter Ulrich, Adam Sandler, Tom Harvey, and Kathleen Maloney, and the model development team, ably led by Dr Christos Mitas, Dr Hichem Boudali, Chris Vos, John Agorgianitis, Dr Malik Awan, and Simon Arnold. We appreciate the RMS team allowing us to use data from the RMS Cyber Loss Experience Database in various chapters of the book. We are of course particularly grateful to Dr Robert Muir Wood, who has created a culture of curiosity and

innovation at the company, from which we all benefit. We are grateful to Hemant Shah, founder of RMS, for his support of research, tolerance of enquiry, and vision for new risk management frameworks, and to Karen White, CEO, for her emphasis on cyber risk analytics in the future of the organization.

We are also grateful to all the RMS clients who have worked with us over the past few years, helping us understand the nature of cyber risk from their experience, perspectives, and claims data.

Cambridge Computer Laboratory, University of Cambridge
We also gratefully acknowledge the inputs and assistance of our colleagues at the Cambridge Computer Laboratory and Cambridge Cybercrime Centre, including Director Dr Richard Clayton, Graham Rymer, Professor Frank Stajano, Professor Ross Anderson, Rob Watson, Dr Alice Hutchings, Professor Jon Crowcroft, and Professor Ian Leslie.

There are a number of hackers and members of the incident response community who contributed to these ideas either directly or indirectly, and either as individuals or as companies doing good work. In no particular order, we thank Sid Rao, Reid Wightman, Matt Erasmus, Erin Burns, Louise Stanhope, Baiba Kaskina, Silje Endsjo, Thomas Dullien, Marion Marschalek, Marie Moe, Alexandre Dulaunoy, Raphael Vinot, Thais Moreira Hamasaki, Aristotle Tzafalias, Arrigo Triulzi, Bruce Stenning, Aaron Kaplan, Thomas Schreck, and Jens Wiesner, with special thanks to Colin Cassidy for going on the full journey.

Finally, but by no means least, we would like to acknowledge the support (and tolerance) of our partners and families in the writing and production of the book. Many thanks, Helen (enjoyed the drinks on the riverbank boring you about hackonomics); Fatma and Mehmet (penguins); and Victoria.

Solving Cyber Risk

CHAPTER 1

Counting the Costs of Cyber Attacks

1.1 ANATOMY OF A DATA EXFILTRATION ATTACK

1.1.1 The Plan

The year 2012 had been good for a small group of cyber hackers. They called themselves '*Rescator*', after the noble and mysterious pirate character in the *Angelique* series of French historical romantic films popular on television in Eastern Europe and Russia. The *Rescator* team specialized in scamming the credentials from credit cards and selling the details for around a 10th of a bitcoin each (approximately $1 in 2012) on sites in the dark web and other black market outlets, such as the Russian 'octavian' marketplace.[1] As they counted their takings in early December 2012, they watched a YouTube meme about the preholiday shopping frenzy taking place in the United States, set to the tune of 'Good King Wenceslas' played on cash registers, a parody of consumerism. *Ker-ching!* Inspired, their planning began in earnest, reinvesting their profits to go for the jackpot: a major theft of US credit card information during next year's holiday spending spree. They could not have known just how successful they would be, and that they were about to commit the biggest theft of credit card data in human history.

1.1.2 The Malware

Rescator began by buying a malware kit from one of the underground forums to create a RAM scraper, similar to other point-of-sale (PoS) hacking malware known as BlackPOS, but significantly more sophisticated.[2] The *Rescator* software later became known as *Kaptoxa*, Russian slang for potato. In the point-of-sale terminals that were standard in US shops in 2013, when a shopper swiped a credit card through the card reader, the information was read from the card's magnetic stripe, and under Payment Card Industry-Data Security Standard (PCI-DSS) rules, the data was encrypted immediately. This protected it at rest while stored on the local device's hard drive, and in transit when it was transmitted to the back-end servers for processing. The 2013 point-of-sale systems had a vulnerability: the card details were read into the computer's temporary memory (RAM) and encrypted while in memory. The malware RAM scraper could detect and copy the credit card details at the microsecond just before the data was encrypted, and send it to a server that *Rescator* would configure to receive the stolen data.

1.1.3 Finding a Way In

Armed with their *Kaptoxa* Trojan horse, the *Rescator* team mapped out a plan to insert it into point-of-sale systems in companies in the United States. They drew up a hit list of the largest retailers that process large volumes of credit card transactions. However, as they went through the list, they found a snag: these big retail companies were all investing heavily in new security systems. During 2012 and throughout 2013, most of the big-name US retailers announced or implemented new installations of malware and data exfiltration detection services – various vendor security systems to prevent unauthorized access to IT systems, to sweep networks for malware, and to monitor traffic on the network to detect suspicious packets that could be data being stolen.

1.1.4 Using Suppliers with Authorized Access

Rescator started to work on finding ways to get around these defenses. Instead of directly targeting the retail companies themselves, they started researching their suppliers and counterparties, particularly anyone who might be granted access into the retailers' information technology (IT) systems.

In September 2013 they hit the bull's-eye. An employee at Fazio Mechanical Services fell for one of their phishing attacks by opening an attachment on an unsolicited email enabling another piece of spyware, *Citadel*, a password-stealing Trojan, to infect Fazio's IT network.[3] Fazio Mechanical Services had an impressive client list of major US retailers in and around Pennsylvania, providing them with refrigeration and heating, ventilation, and air-conditioning (HVAC) systems, servicing their cold stores for frozen foods, and managing the energy usage and temperatures of large retail outlets. Fazio had access into the IT networks of its customers to enable it to monitor, troubleshoot, and control their refrigeration plants and HVAC systems.

Most significantly of all, the Fazio customer list included stores belonging to Target Corporation, a major discount store operator and second only to Walmart in US retail size. Target operated 1793 stores across 47 states in 2013, and had revenues of $72.5 billion.

1.1.5 Installing the Malware

Using their password-stealing Trojan, the *Rescator* team was able to obtain the credentials of the Fazio operators who routinely logged in through the firewall of Target Corporation into its IT network to monitor the Target refrigeration and HVAC systems. During the Thanksgiving holiday in November 2013 when most of the company was closed, they used these access codes to log in to the Target IT network and install their RAM-scraping malware on a few point-of-sale systems in Target stores. They took a couple of days to check that it worked, carried out systems checks, and waited to see if it would be detected. The *Kaptoxa* malware was sophisticated enough to be invisible to some of the best anti-malware systems in use at that time. Target was running 40 different commercial anti-malware tools, sweeping its networks and point-of-sale systems, and looking for any software that matched suspicious signatures. None of the systems identified the *Kaptoxa* installations as malicious.[4]

When the *Rescator* team found that their software had succeeded in evading the anti-malware sweeps, they returned and overnight pushed their malware to as many of Target's point-of-sale systems as they could reach.

1.1.6 Harvesting the Data

The pre-holiday season was indeed busy. Shoppers flocked into Target stores for their holiday gifts, appliances, and supplies. In a period from November 27, to December 15, 2013, the *Kaptoxa* malware on the point-of-sale systems in Target stores across the United States captured the details of transactions from 40 million debit and credit cards. An additional overlapping customer database that contained names and addresses of 70 million people was also stolen. It was the largest cache of credit card data that had ever been stolen.

The *Kaptoxa* malware cached the data it was stealing locally at each point-of-sale terminal. Every seven hours it checked the local time, and if it was between 10 a.m. and 5 p.m. it would send the data over the busy network traffic to an internal host on a compromised server inside the Target network. From there, the *Rescator* team used a series of remote file transfer protocol (FTP) transfers to retrieve the intercepted information, amounting to around 11 Gb of data. The stolen data transfers went to a number of 'drop' locations – servers in Russia, the United States, and Brazil that the *Rescator* gang controlled.[5] These were computers in unsuspecting organizations that had also been hacked, giving the gang the ability to store the data there temporarily before moving the data on to a destination source, and masking their tracks.

1.1.7 Selling the Stolen Data

The gang moved quickly, trying to sell the stolen credit card details before the hack was discovered. They made the data available on their own marketplace website, as well as auction sites on the dark web and black market private dealerships. They sorted the stolen cards into categories, offering them for sale in blocks, such as 'Tortuga' and 'Barbarossa'. These were bought by other black market fraudsters to create new counterfeit cards mainly for use in shopping in stores for items than could be easily resold, classifying them by ZIP code to enable the fraudsters to shop locally like the real card owner to lessen suspicion. These card details contained full transaction information and verification details and were offered for prices around $20. They also offered non-US cards, chip-and-PIN (Europay, MasterCard, Visa [known as EMV cards]), and platinum or premium cards that were sold at higher prices, up to $120.[6]

1.1.8 Buy Back and Discovery

The sites where credit card information is offered for sale are routinely monitored by fraud detection officers from the card companies and major banks. It is a poorly-kept secret that the banks themselves buy back some of the card details on offer to take them off the black market and protect their cardholders. Banks may in fact be some of the best customers of credit card hackers. Around December 15, the bankers who were buying back their cardholders' details noticed that large volumes of new credit card details were appearing on the black market, with one thing in common – they had all made a purchase at Target in the past few days. They called Target. Some of them also spoke off the record to a cyber security journalist, Brian Krebs, who may have broken the news story on his blog on December 18.[7] Target's forensic teams and their security consultants identified and removed the malware from the infected point-of-sale systems in a few hours, and began a full internal systems security audit and investigation. The investigation took many weeks to complete.

1.1.9 Disclosure

Target Corporation made a formal announcement of the data breach on December 19, 2013, saying that the matter was under investigation and that Target was now working with law enforcement authorities and financial institutions.[8] US state regulations for the protection of personal data require companies that have a data breach to disclose it publicly and promptly, and to take steps to notify the individuals whose personal data has been compromised. Target's website providing information about the breach, and its customer service hotlines, became overloaded as the company began to assist customers with questions about whether they might have been compromised and what to do about it. Target had to hire additional customer service personnel to deal with the surge in worried calls.

1.1.10 Customer Management

The first question of any of Target's customers is 'Was my card information stolen?' Not all of the point-of-sale terminals had been infected, and it wasn't initially clear how long the interceptions had been going on. The forensics to understand the extent, duration, and transactions that might have been compromised took several days to unravel. Target worked with banks to have millions of compromised cards stopped and reissued.

Customers' main fears in response to having their card and personal details stolen are that their cards could be used in fraudulent payments, that they could lose money from their bank accounts, and that their own credit histories and ratings could be impacted. Target offered credit monitoring for a year to each person whose details were stolen. There is also a potential for a secondary fraud, where a criminal armed with the stolen personal details contacts individuals and tricks them into false payments or more disclosures. Target offered advice to counter secondary fraud, including changing account passwords and insisting on ring-backs for unsolicited phone calls.

1.1.11 Target's Costs

Target's direct costs from the breach reached over $200 million, and took several years to accrue. In 2015, Target paid out $40 million to banks and credit unions that lost money, paid out to buy back card data, or incurred further loss resulting from the data breach.[9] A consumer class action was settled at $10 million to establish a fund for victims of the data breach, with individual customers able to claim up to $10,000 if they could provide satisfactory evidence of their losses and costs incurred. Victims were also allowed to apply for up to two hours of their 'lost time', billable at $10 per hour. Allowable costs include reimbursed charges on their credit cards, fees for hiring a professional to correct a credit report, late and declined payment fees, and other costs incurred as a consequence of the breach.[10]

Target came to a $18.5 million collective settlement for the regulatory fines with the state attorney generals in the 47 states where it had stores in 2017, the largest payout being $1.4 million for California, with 7.7 million affected Target customers. An additional component of the regulatory settlement ensured that Target implemented a comprehensive information security program, overseen by an independent, qualified third party, and employed a chief information security officer, reporting to the chief executive and board.

1.1.12 Strategic Impacts on Target Corporation

The data breach had additional consequences for Target Corporation. The chief executive resigned in May 2014, following the chief information officer in March. Profits for the quarter following the breach dropped by 46%, and contributed to a reduced profit for the year.[11] The damage to the company's reputation caused a reduction in visits to its stores. Target attempted to offset this with a 10% discount offer immediately after the breach, but customer confidence was not easily restored, and Target continued to struggle for some months. Consequential costs of the impact on Target's revenues in the year that followed the breach are harder to gauge, but some estimates suggest it could have been between $1 billion and $2 billion, more than five times the direct costs and between 1.4% and 2.8% of Target's annual revenue.

Share prices dropped several times in response to various stages of disclosure about the breach, initially falling 11% in the weeks after the breach, recovering around 7% with a comforting financial outlook reporting in the following quarter of 2014, and falling again with various settlements and payouts as they were resolved over the following years. Some analysts see the data breach as having undermined confidence in the company's strategic direction, as it tries to promote in-store experience to compete with e-commerce retailers.

1.1.13 And the *Rescator* Team?

Nobody was ever caught or prosecuted for the Target cyber hack. Two petty criminals were caught in possession of 112 derived fraudulent credit cards, but to date none of the perpetrators. Target Corporation was not the only victim of point-of-sale malware during the holiday period of 2013. Neiman Marcus and three other retailers reported credit card intercepts. The illegal marketplaces, including *Rescator*'s own marketplace, where the stolen credit cards were offered for sale, were abandoned shortly after the publicity broke.

It is difficult to know how much money the *Rescator* gang made from the operation. A conservative estimate might be $50 million: a long way from the $2 billion it cost Target. The *Rescator* gang, named for a mysterious pirate, has vanished with its treasure, back to the seven seas.

1.1.14 Fallout

The consequences of the Target data breach have been profound. Point-of-sale systems have been largely redesigned, and the key vulnerability has been addressed. It is no longer acceptable practice to have point-of-sale systems accessible through the same IT network as HVAC controls and other general activities accessed by a broader, less secure community. Data encryption practices have become more widespread, and verification processes have become more secure. Hacks like these have accelerated the take-up of chip-and-PIN (EMV) credit card technology in many countries of the world, which cuts card-related theft by up to 70%. It is highly unlikely that a cyber hack using the same exploits and techniques as the Target data breach will be seen again.

But it doesn't mean that new techniques won't be used to carry out a similar scale of cyber attack in the future.

1.2 A MODERN SCOURGE

1.2.1 Types of Cyber Losses

The Target Corporation data breach in 2013 was a high-profile cyber attack that caused a variety of losses and business impacts on one of the largest companies in the United States. However, it was only one of many successful cyber attacks that year; 2013 was a record year for data exfiltration events in the United States. There were 31 reported breaches that year where a US company lost a data set of a million personal records or more, and over 640 US companies reported a loss of more than a thousand personal data records.

Historically, 2013 looks to have been a peak year for the number of US data breach events, as US companies have improved their data security, and incident rates have dropped in the years since. However, all over the rest of the world, the number of data exfiltration incidences has been steadily increasing – the types and severities of attacks seen in the United States since 2005 are now occurring in many other countries.

Data exfiltration attacks are only one of the ways that cyber attacks cause loss to individual organizations and to society as a whole. Most organizations of any significant size report having to deal frequently with cyber incidents of many different types – attempted attacks, probes, phishing approaches, suspicious software detection, unusual network traffic. Sometimes these result in a 'cyber loss' – the organization is compromised in some way and incurs costs through payouts or business disruption. Of course even dealing with attempted attacks has a business cost (which we will come back to later), but in general we refer to a 'loss' as being a cyber incident that results in an organization having a significant unexpected financial payout or an episode of business disruption that prevents the generation of expected revenues. The next chapter describes and defines the losses that can be caused by the various types of cyber incidents, including data exfiltration, so costly to Target, as well as contagious malware, extortion, financial thefts, denial of service attacks, failures of networks, and outages of providers. We also try to define the range of severities of these different types of loss, and a threshold of severity that we might consider as significant, which we use to define 'loss' incidents in this book. In our third chapter we describe the loss processes that can occur from cyber attacks to physical systems and devices.

1.2.2 The Direct Payout Costs of a Cyber Attack

A cyber attack that succeeds in penetrating the defenses of an organization can cause losses in various ways. As illustrated in the example of the data exfiltration attack on Target Corporation, the $200 million in direct costs consisted of losses from several different sources.

A company suffering a cyber attack can expect to incur direct payout costs in a number of different areas, depending on the type of attack and the magnitude and characteristics of the attack. Costs of different types of attack are described in more detail in Chapter 2. Types of direct payout costs include:

- The response and forensics costs of the IT security team, both internal personnel and typically involving external consultants, that has to diagnose what happened as quickly as possible and render the system safe from further exploitation. New technology, equipment, software, and systems may need to be purchased to remedy vulnerabilities.
- Compensation for people whose personal data is compromised, including costs of notification, managing their enquiries and providing customer support, providing credit watch services, and payouts for any losses these individuals may suffer.
- Fines that may be imposed by regulators.

- Legal costs to defend any litigation that might be brought against the company, including the costs of settling the action or losing the case and paying damages or even punitive awards.
- Losses from the theft of financial assets – currency, transfers, trading value – which is the motivation behind many attacks.

1.2.3 Operational Disruption Causing Loss of Revenue

Costs are also incurred to the affected company from the disruption to business operations resulting from the attack, particularly lost revenues from commercial activities that are unable to be performed. Operational disruption can last for several hours or days and affect many parts of an organization. Surveys of corporate security executives show that breaches impact more than a third of a company's systems in around 40% of cases and more than half of systems in 15% of cases. They disable operational activity, including revenue generation, for more than 9 hours in 35% of cases and for durations of 24 hours or more in 9% of cases.[12] Operational disablement of systems can result in revenue loss to many different business processes, and each organization is different. Losses can occur from suspending customer purchasing activities, such as e-commerce or point-of-sale technologies; provision of services, such as hosting applications; fulfillment of orders; manufacturing or creation of products for sale; and interruption of the business process supply chain. These losses of revenue that can be directly attributed to the interruption of systems caused by the cyber attack are often included in direct costs estimates of a cyber attack.

1.2.4 Consequential Business Losses from a Cyber Attack

The consequential business losses from a data breach can be more severe than the direct costs. The company's reputation is damaged. Senior executives resign. Customers lose trust and transfer their business elsewhere. Revenues dip, and market share is lost to competitors. Studies show typical churn rates of around 7% of a company's customers after a data breach, and 31% of consumers have discontinued a relationship with an organization that has suffered a data breach.[13] Around a third of companies that experience a breach have reportedly suffered revenue loss, around 12% reported losses greater than 20% of their annual revenue, and just over 1% lost more than 80% of their annual revenue.[14] These companies also reported customer desertion and significant losses in business opportunities as a result of the breach.

Companies that suffer a costly cyber attack typically see their stock prices marked down.[15] Analysis of historical cases shows that companies see their share prices reduced by an average of 5% after a data breach attack.[16] Stock price reductions can be short term while the market waits to see how the company will be affected, but in cases where the consequences prejudice the organization's business model or long-term profitability, investors can mark them down significantly and for a long period.

A major cyber attack can cause a company to have its credit ratings downgraded.[17] Companies seen as a credit risk lose suppliers as well as customers, and find it more expensive to borrow capital and fund their cash flow. Credit rating downgrades indicate to the public that a company is in distress, and can hasten a company's decline and threaten its viability.

These combined effects have meant that some companies have declared bankruptcy following cyber attacks.[18] Companies that have had their intellectual property (IP) stolen have found themselves outcompeted in the market, leading to their long-term failure.[19]

The viability of a company can also be threatened in other ways if the consequences of the attack are severe enough. There have been cases where class-action litigations brought against a company for its data breach liabilities far exceed the capital valuation of the company.[20] Companies have been devalued in merger and acquisition negotiations because they suffered data breaches.[21] The impact of experiencing a data breach can go far beyond the direct costs, and can impact the brand, the reputation, and the viability of the company itself.

1.2.5 Cyber Attack Economic Multipliers

Finally, the effects are not isolated to the individual organization that is attacked. The consequences are also felt by the company's suppliers and trading partners, investors, financiers, and other counterparties. They in turn sell less to the affected company and reduce their revenues, or they lose part of their investment value, loans returns, or earnings. Companies are part of a network of commerce, and the failure or reduction in performance by one company has consequential effects on others. Economists term this the multiplier effect, or 'financial spillover'. Cyber attacks have a clear multiplier effect on the economy as a whole.

In an analysis that the authors published in 2014, we assessed the economic multipliers of cyber attacks by tracking the connectivity of companies in the global economy.[22]

Figure 1.1 shows a network diagram of around a thousand of the largest enterprises in the global economy, sized by their annual revenue, with the

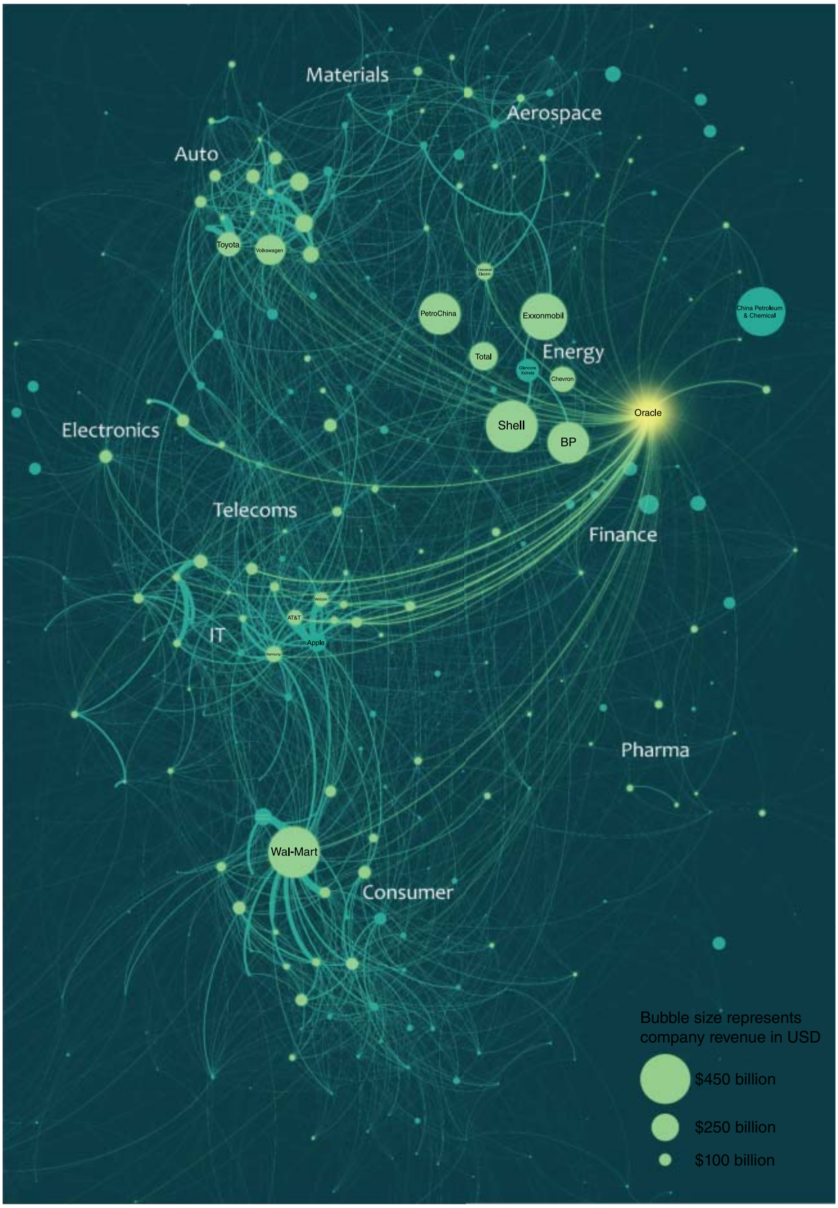

FIGURE 1.1 Trading interconnectivity of major companies in the global economy. Cyber losses can cascade through the economy to create a multiplier effect for economic costs. Oracle, a market-leading provider of databases, is highlighted to illustrate an example of the key role played by providers of information technology in the global economy.
Source: CCRS (2014a).

trading relationships between them shown by the thickness of the line, and the direction of payment flowing counterclockwise. The reduction in annual revenues of any of these large corporations has a consequential effect in reducing their requirement from their suppliers and curtailing their ability to purchase from trading partners. Fluctuations in quarterly reported revenue (from whatever cause) affect trading partners when change exceeds around 10% of expected annual revenue, with greater increases having disproportionately larger effects on their counterparties. The number of trading partners and the depth of trading relationships influence how these impacts spread through the trade network. For a medium-to-large company losing around 20% of its annual revenue (something that occurs in around 12% of data breach cases), we estimate the economic multiplier to be around 1.6 – i.e. the suppliers and customers collectively lose an additional total of 1.6 times the losses that the company itself loses in a cyber attack.

For example, if a company with a $1 billion turnover suffered a data exfiltration event of 20 million personal records, it would face direct costs of around $50 billion, combined with consequential business costs by subsequently losing around 20% of annual revenue ($200 million), and its suppliers and counterparties suffering collective losses of 1.6 times this ($320 million). The total cost of this example of a single data breach on the overall economy is $570 million, more than 10 times the direct costs. Fully recognizing the economic costs of cyber attacks is important in assessing the value of measures to reduce cyber risk.

The economic multiplier increases if several companies suffer losses at the same time. If several of the impacted companies share a supplier, then they may all reduce their volume of orders to that supplier and cumulatively inflict a large enough loss to the supplier to cause it to have financial difficulties, with knock-on effects to its own suppliers and trading partners. This cascade of effects through the economy is known as a systemic shock. This is what makes cyber catastrophes such a concern.

1.3 CYBER CATASTROPHES

A cyber catastrophe is an event that causes substantial losses to many organizations. For many years people have predicted a ‘cyber 9/11’, a ‘cyber Pearl Harbor’, or a ‘cyber Black Swan’. These predictions identify the issue of the potential for strategic surprise from an unexpectedly large cyber catastrophe.

We define a cyber catastrophe as a cyber incident (a criminal campaign, a malware attack, or a major malfunction) that results in significant direct costs and consequential business losses to many (more than 10, but could be many thousands) multinational or very large premier organizations, or very many (more than a thousand) small and medium-size enterprises.[23] In addition to being a shock event, a cyber catastrophe can also be a general trend of slow losses and reduced economic revenues.

1.3.1 *NotPetya* and *WannaCry* Cyber Catastrophes

NotPetya and *WannaCryptor* malware attacks are profiled in more detail in the next chapter. These are examples of cyber catastrophes at the relatively low end of the potential magnitude scale.

The *NotPetya* virus release in June 2017 penetrated at least 8,000 computer networks, infecting many hundreds of thousands of individual devices, in organizations across 65 countries. More than 300 public companies declared losses to their quarterly results as a result of their infections from *NotPetya*, several reporting losses of hundreds of millions of dollars. The direct and consequential business losses to the infected organizations is estimated to have exceeded $10 billion.[24]

The *WannaCry* ransomware attack in May 2017 was more widespread, but less severe overall. It caused more than 300,000 infections, mainly smaller businesses, but the impact did disrupt the operations of some major organizations, including healthcare providers whose patients were put at risk. The combined losses to the infected businesses are estimated to have been several billion dollars.[25]

1.3.2 Near-miss Cyber Catastrophes

These events and others in recent history demonstrate that cyber catastrophes have the potential to disrupt many businesses worldwide simultaneously. In fact, these recent events can be seen as ‘near misses’. They were bad-enough events, but could have been even more severe with only minor changes in the way they occurred. Our counterfactual analysis of the *WannaCry* timeline, described in more detail in the next chapter, suggests that the *WannaCry* event could have been many multiples of its actual cost if it had occurred three months earlier and had not included a kill switch in its software design.

There have been several other cyber events that had the potential to become truly systemic, and to inflict widespread disruption and business losses on thousands of organizations. These might be considered as early warning indicators of potential cyber catastrophes. They include:

- A cyber heist operation on banks by penetrating the Society for Worldwide Interbank Financial Telecommunication (SWIFT) financial transaction system impacted more than a dozen national and international banks (August 2016), resulting in the theft of $81 million, but the theft of a billion dollars was attempted and narrowly thwarted. The heist compromised a secure ‘network of trust’: the SWIFT financial system, used by 11,000 banks, any or all of which could potentially have been robbed.

- A distributed denial of service (DDoS) attack on Dyn, a provider of Domain Name System (DNS) and internet optimization services (October 2016), caused disruption to thousands of its internet service company customers in Europe and North America. The attacks caused service losses of several hours during a single day to many leading e-commerce businesses. It highlighted the vulnerability of DNS infrastructure supporting the digital economy, and indicates the potential for cyber catastrophes to disrupt global e-commerce.
- An outage of the Amazon Web Services (AWS) Simple Storage Service (S3) for five hours affected 148,000 websites and nearly a quarter of all AWS cloud users (March 2017). Cloud service providers (CSPs) like AWS, Google Cloud Platform, Microsoft Azure, and IBM Bluemix tend to have very low failure rates, but the dependency of so many businesses on these leading CSPs means that if there were to be a failure then there is potential for a CSP outage to disrupt many thousands of cloud-reliant businesses.
- The release of stolen National Security Agency (NSA) and Central Intelligence Agency (CIA) cyber toolkits by a cyber hacking group calling themselves *ShadowBrokers* was a game changer by making highly professional cyber weaponry available to less skilled amateur hackers (August 2016 and April 2017). The releases included 15 ‘zero day’ exploits for common software in use, and 24 other tools. The toolkit provided the keys to unlock the firewalls of 30% of all global corporations. These exploits were incorporated into the malware of *NotPetya* and *WannaCry*, but also illustrates how tools could suddenly become available to bypass the apparently impenetrable security systems operated by most of the major international companies.
- A security bug in widely used open-source database MongoDB meant that ransomware *Harak1r1* was able to access data in ‘tens of thousands’ of MongoDB installations and deny them access until payments were made (January 2017). ‘Many’ MongoDB servers were reported extorted. This raises the specter of industry-standard software in use by large numbers of organizations suddenly failing or causing losses simultaneously as a result of an internal software bug or vulnerability.

There has not yet been a truly catastrophic cyber event that has cost the economy hundreds of billions of dollars. It is human nature to dismiss