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

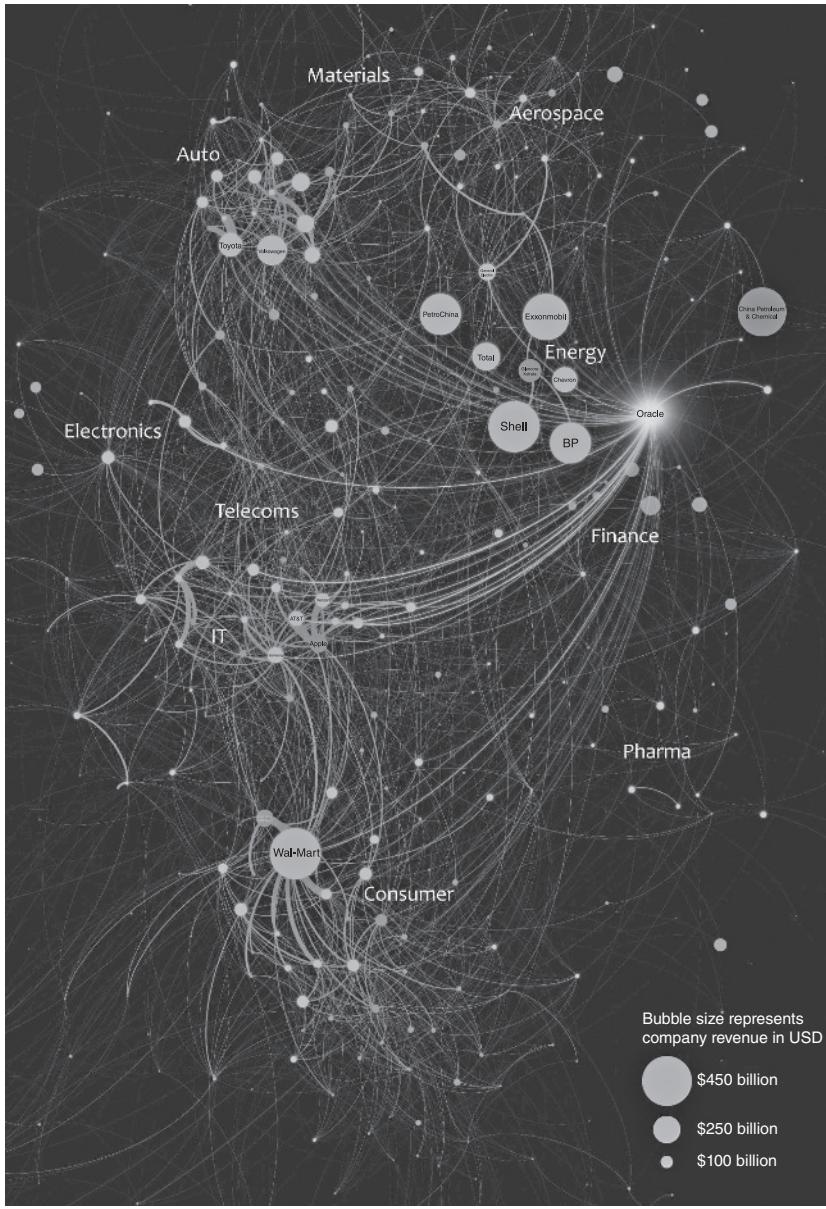

FIGURE 1.1 Trading interconnectivity of major companies in the global economy. Cyber losses can cascade through the economy to create a multiplier effect for economic costs. Oracle, a market-leading provider of databases, is highlighted to illustrate an example of the key role played by providers of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

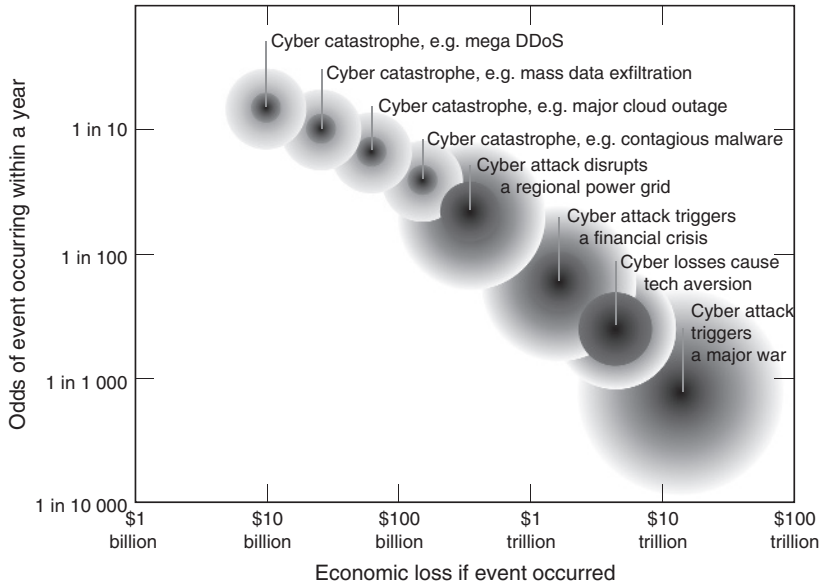

FIGURE 1.2 Global cyber risk: likelihood of loss occurring from cyber attacks. Source: Authors (2018).

possible dangers before an event has actually occurred. But there are reasons to believe that future cyber events are possible that could inflict individual costs of hundreds of millions or even billions of dollars to thousands of major businesses, and inflict crippling losses on large numbers of small and medium-size enterprises. These events, described in the following section and illustrated in Figure 1.2, would have a heavy impact on the economy and on society in general. The likelihood of a future societal catastrophe from cyber attacks is one of the strongest justifications for taking more action to solve cyber risk.

1.3.3 Is Cyber Threat Systemic?

The concept of cyber threat having the ability to scale up to cause systemic losses to thousands of organizations, with potential to cause catastrophic consequences for our society and our economy, is better accepted now, but the recognition of this potential is relatively recent. This led people to assume that cyber threat is predominantly characterized by separate loss events at individual organizations, and is limited in its ability to propagate more broadly. Only a few years ago there was still debate about whether the

emerging threat from cyber risk is truly systemic, and the extent to which cyber risk could scale.[26]

Part of the authors' research has been assessing the risk of extreme events for regulators, governments, insurance companies, and corporations.

1.3.4 Potential Cyber Catastrophes

There are several ways in which cyber catastrophes could occur. We have developed plausible scenarios that are used as stress tests by organizations in their cyber protection planning. In the next chapter we include a 'severe but plausible' cyber catastrophe scenario for each of the cyber loss mechanisms described. It is possible that next year could see the number and severity of data exfiltration incidents increase by an order of magnitude, as a result of a concerted campaign by criminals armed with a new toolkit of exploits to penetrate the security systems of multiple multinational companies.[27] Another potential cyber catastrophe scenario is a contagious ransomware virus that achieves infection rates much higher than anything previously seen, and is both destructive and disruptive to business activities across large numbers of organizations, of all sizes and nationalities.[28] It is possible that denial of service attacks could increase in volume and intensity and target major e-commerce platforms to immobilize many of them for much longer than has been achieved before.[29] A major cloud service provider could suffer an outage on a scale and duration that exceeds anything previously recorded, causing hundreds of thousands of its customers difficulties in sustaining their cloud-dependent business activities.[30] Industrial control systems could be hacked, damaging and disabling manufacturing and processing operations in large numbers of plants.[31]

For each of these, the analysis considers the practical constraints of attack vectors, the capabilities of attackers, how many organizations could potentially be impacted, and what limits there might be to the severity of the consequences. In each case there are typically factors that constrain the number of organizations that a potential cyber loss process might impact. For example, to penetrate a large number of companies, a 'zero day' exploit operates on a particular software system, so only the companies operating that software system would potentially be affected by that exploit. The market share of industry-standard software systems becomes a determinant constraint on the number of organizations that might be affected. Other constraints include the expected response by the security community to detect, protect, and respond quickly to limit the extent of the impact of any event.

These scenarios estimate the numbers of affected operations and loss costs across the population of organizations in an economy such as the United States. Although large numbers of small and medium-size organizations are affected in these scenarios, the main driver of cost to the economy is the impact on large and premier companies. Scenarios where 15–20% of large companies are impacted are feasible in several of the loss processes. It is possible to envision extreme scenarios where as many as 50% of large companies could be hit, under pessimistic assumptions about the resources and skills available to the attackers, and how different defense and response strategies by the community of security specialists might play out. These scenarios result in direct loss and operational disruption costs to the population of US businesses of many tens, and in some extreme cases hundreds, of billions of dollars. These catastrophe scenarios would not be confined geographically to the United States. Similar losses could be expected in companies affected in other developed economies, including Europe, Australasia, India, China, Japan, and Southeast Asian markets. The direct costs would be exceeded by the consequential losses of earnings to these businesses, and as noted earlier, by the multipliers on the economic impact from their effects on suppliers and customers and the economic trading network.

1.3.5 Cyber Catastrophes Could Impact Infrastructure

There is even greater potential economic impact from cyber catastrophe scenarios that target key components of the infrastructure, rather than the organizations themselves. We have analyzed scenarios where cyber attacks could disable the power supply in different countries. In 2014 and 2015 when we published these analyses, the idea that foreign agents could potentially attack the power supplies in another country appeared far-fetched, until cyber attacks on the Ukraine power grid in December 2015 left 80,000 people without electricity.[32]

A potential cyber attack could damage and disable multiple power generators in the United States electricity grid. The US grid is compartmentalized into interconnected regions, and the spinning reserve capacity needs to be depleted before cascading failure can occur. A cyber attack that used known vulnerabilities to damage 50 generators in the most populous Northeastern region of the United States could result in loss of power to 90 million people, with reconnection for most of them taking a day or two, but full restoration taking between two and four weeks.[33] This results in disruption to businesses in the region, most significantly on the commercial and industrial sectors that are most reliant on power for their business activities. We estimate the total economic impact of such an event at between $243 billion

and, under extreme pessimistic assumptions, over a trillion dollars of lost output from the US economy.

A similar analysis of a future cyber attack on the power distribution system of the United Kingdom, a much smaller country and economy and with a different type of power grid architecture, produces a regional power supply outage that affects between 9 million and 13 million electricity customers.[34] The knock-on effects include disruption to transportation, digital communications, and water services. The attack results in an estimated loss of between $70 billion and $628 billion to the UK economy.

These scenarios demonstrate that cyber attacks on infrastructure have the potential to generate very substantial shocks to the economies of the countries attacked, and are among some of the most severe consequences of cyber risk to our society.

1.3.6 Could a Cyber Catastrophe Trigger a Financial Crisis?

Cyber attacks and technology errors could potentially trigger a future financial crisis. Flash crashes have been seen on trading exchanges as a result of trading algorithm malfunctions, cryptocurrencies have been hacked and destabilized, and major financial trading systems have been cyber attacked and plundered. There are genuine fears that a future cyber attack or cyber-enabled fraud could trigger a confidence crisis in the markets that would spread through the financial system and result in a worldwide financial crisis with severe negative impacts on the global economy.[35] Others disagree, arguing that the financial system is resilient to shocks of this type.[36] Even a small financial crisis can wipe hundreds of billions of dollars of value off the market capitalization of listed companies, and can result in reduced output from national economies for years.[37] If a major cyber attack succeeded in stealing from large numbers of financial services companies and caused a crisis of confidence by investors in their banks or the values of their financial assets, then the ensuing financial crisis could be more costly and disruptive to society than many other types of cyber incidents.

1.3.7 The 'Cyber Catastrophe' of Tech Aversion

One of the worst outcomes from high levels of continued cyber losses or severe cyber catastrophes is the possibility that the general public might lose confidence in information technology, and distrust its ability to deliver benefits that are greater than its risks of security breaches. Surveys of consumers

show that there is ambivalence about trusting technology. Many see the advantages, but are wary about third parties failing to protect or respect their data privacy. They fear cyber attacks that will cause them losses and so are reluctant to rely on digital bank accounts, transact online, or embrace further innovations that could be to their benefit. Various names have been used for this phenomenon, including 'tech aversion', 'e-luctance', 'cyber malaise', and 'technophobia'. This could be responsible for the most severe of all of the economic costs of societal cyber risk by threatening future productivity gains from the digital economy.

The past half-century of economic growth has been driven by a combination of factors, including globalization of trade, financial deregulation, innovation, education, and rapidly improving productivity levels. Global economic output doubled in the period between 1970 and 1985, and has doubled again from 1985 to present-day levels, marking the period of fastest economic growth in human history. This has delivered unprecedented prosperity for the mainstream populations of the developed economies. A major contribution to this economic growth has been the improvement of productivity delivered by information technology. Although there are different views on the contribution of IT to productivity, some economists have suggested that up to 40% of US productivity growth between 1995 and 2002 can be attributed to IT.[38] IT is an enabling technology that allows businesses to improve their output at decreasing costs.

Many analysts predict that we are about to embark on another period of productivity improvement – a 'fourth industrial revolution' – enabled by Big Data, artificial intelligence, robotics, and machine learning. Phrases like 'data is the new oil' underpin a view that information is increasingly enabling accelerated economic growth.

Our analysis of this scenario considered the sectors of the economy that would most suffer from tech aversion and rated the IT business process criticality of operations to key technologies.[39] Productivity losses, consumer confidence, capital investment levels, and consumption indexes were stressed in macroeconomic modeling of the consequences of a 'tech-averse' future. The global economy lost between $4.5 *trillion* and $15 *trillion* over a five-year projection, depending on the assumptions made.

1.4 SOCIETAL CYBER THREATS

1.4.1 Cyber Threats to Democracy

Cyber activities and the capabilities of hacker groups not only add a significant burden of cost to our economies but also pose a threat to the functioning

of our society. Fake news, chatbots, and the manipulation of social media are now commonplace in democratic election campaigns, and may have influenced the outcome of key elections.[40] The permeation of false rumors can manipulate public opinion, electorates, stock prices, and currency markets. Politically motivated attacks and manipulation can undermine the legitimacy of our democratic processes and our confidence in truth, the veracity of sources of information, and our ability to differentiate between realities and lies. As marketing agencies increasingly set up botnets to endorse products through false accounts in social media, and fake news reports try to manipulate financial markets, the public becomes increasingly confused, distrusting, and wary of information. This has a social cost and will be rectified only with better codes of digital ethics, abilities to detect and differentiate veracity, and capabilities to deter and prevent interference in democratic practise.

1.4.2 The Cyber Threat of Triggering War

The best-resourced cyber teams are state-sponsored cyber warriors who are increasingly active in testing their techniques by penetrating the organizations of other countries. In Chapter 5 we list some of the 91 national cyber operations teams that are active today. At least 20 of these are potentially antagonistic to Western democracies.

One of the greatest threats that cyber capabilities pose is the potential to trigger conflicts that could rapidly escalate into conventional military warfare. Cyber intrusions into private-sector or non-military organizations have occurred where the perpetrators are suspected to be foreign state–backed operations teams. Typically these ops teams are spying on industrial secrets, stealing funds for impoverished regimes, exploring weaknesses in military systems, and probing and learning about vulnerabilities in the infrastructures and economies of their potential future enemies. So far, disruptive and damaging cyber attacks by foreign operatives are tolerated by national security agencies – partly because of the difficulties of attributing with certainty who carried out the attacks. Most nations that suffer incursions from the cyber ops teams of foreign countries have developed offensive capabilities for retaliation, and for first-strike options.

It is still of course against international law for cyber ops teams to carry out attacks that damage assets in another country, but several western democracies, including the United States, UK, Germany, and Australia, have now passed laws giving their own cyber ops teams the authority to carry out cyber offensive activities in foreign jurisdictions. Some of these have gone public with their capabilities, including the ability to make another country's warplanes, ships, and missiles malfunction, and cripple national

infrastructure and the data and communications systems of potential enemies.[41] In 2016, NATO decided that a cyber attack on any member country would constitute an attack under the provision of Article 5, the mutual defense guarantee, that would trigger collective response, including options for retaliation with conventional military weapons.[42]

For many decades, the military dominance and balance of the superpowers has largely prevented armed conflicts – the frequency of international wars is at its lowest for several centuries. However, cyber power has changed this equation and is highly asymmetric. Nations like North Korea that cannot match the military firepower of the superpowers, now have extensive cyber ops capability. The existence of national cyber ops teams, both as an extension of military capability and as national security protection, makes the possibility of international cyber retaliatory strikes a lot more likely, and these have the potential to rapidly escalate into a conventional military conflict. Future geopolitical conflicts are likely to have an entire theater of war in cyberspace. Much of the conflict in Ukraine from 2014 onwards has featured cyber attacks on military and civilian infrastructure and data systems targets that support the military offensives, with suspected Russian involvement. The Ukraine conflict is cited as a template for future wars.

If cyber attacks can trigger wars between nations, then this may be the biggest risk of all. The greatest risks to society, the economy, and our well-being overall have historically come from the threats of war. Wars in the last century alone have caused millions of deaths, the loss of trillions of dollars of economic output, and the biggest disruption to society. In our analysis of possible costs to the global economy from even a contained conflict between two advanced economies, our estimates ranged from $17 trillion to $32 trillion.[43] If cyber capability and our tolerance of low-level cyber attacks by one country against another make wars more likely, then the societal risk from cyber threats has a longer tail – i.e. the extreme severity of low-likelihood outcomes might be more costly to society – than people might realize.

1.5 CYBER RISK

1.5.1 Risk Terminology

Risk means the likelihood of loss. We quantify risk by assessing the probability of a specified severity of loss within a given time period. For example, the odds of a large US healthcare company experiencing a cyber attack that causes it direct costs of $10 million or more in the next 12 months would

be around 1 in 100. Its chances of having a more severe event that causes a higher level of cost, say $100 million, are much less likely: around 1 in 700. The more severe the event, the less likely it is. There is a continuous scale from low levels of cost to the most severe, and at each level of loss there is a corresponding range of likelihood, with the low levels being most common and the most severe being least likely.

This relationship between loss severity and likelihood, known as the 'risk profile', the 'frequency-severity distribution', or the 'loss exceedance probability curve', is the measurement of risk, and is how risk managers assess and think about risk. This is how the term *risk* is used within this book. We use the term *threat* to mean the likelihood of an attempted cyber attack on your organization (and levels of attacks going on in the environment), and in risk terminology your 'vulnerability' means the chances of your company suffering a loss from an attempted attack (which is slightly more general than the IT security technical meaning of a 'vulnerability' being an error in software that can be exploited by a hacker).

The risk profile can be used to assess the average loss rate over time that you might expect from all the different likelihoods and severities of future cyber attacks. This is known as the 'expected loss', and is the equivalent of how much you would need to put away in savings each year to pay for all future cyber losses. Perhaps more importantly, it tells you the likelihood of an event occurring that would result in an 'unacceptable' level of loss to your organization.

1.5.2 A Framework for Risk Assessment

It is useful to calculate your risk profile in this way, even though there are large uncertainties in the estimation of likelihood of future cyber losses. Risk varies over time, and for different environments in which organizations operate. Most organizations experience many attempted cyber attacks, and with good security systems in place, their vulnerability rates are low, so the chances of experiencing a cyber loss in any given period are relatively small. However, some cyber attacks do succeed and losses occur. We note the losses that occur across the entire population of organizations, and observe how often and how severely they happen to companies that are similar to yours, even if you yourself have not experienced a loss. You could experience a future cyber loss as a result of unknown vulnerabilities in your trusted systems, attacker ingenuity using techniques you have not foreseen, failures in your security processes, human error, malicious insiders, alignment of multiple unexpected events, or other unpredictable circumstances. We try to capture this in the framework of assessing the

risk profile of the frequency and severity of potential cyber losses for an organization.

1.5.3 Risk Tolerance of Your Organization

Some companies may tolerate the occasional minor loss from cyber attacks. In fact, it may be too costly relative to the value to make an organization invulnerable and to prevent any cyber loss occurrence at all. But most companies want to avoid having a severe loss above a certain threshold, particularly one that will cause reputation damage, lead to missing earnings targets, materially damage the balance sheet, trigger a rating downgrade, or threaten the viability of the organization itself.

The point of estimating a cyber risk profile for an organization is to assess the value and effectiveness of measures taken to reduce the risk of an unacceptable loss. Each organization has its own risk tolerance and, implicitly or explicitly, manages its businesses to this tolerance, investing in security or imposing procedural change to reduce risks that are unacceptable. We believe that risk management decisions should be based on objective assessments of risk, and be as evidence-based as possible. You should be able to estimate how various security measures and risk mitigation processes will affect your risk profile, and to justify their implementation by how much they will reduce the risk of unacceptable loss. This book sets out a framework for risk assessment and tries to provide information that will help you make some of the estimates you need to assess the risk profile of your organization.

Cyber risk profiles vary significantly from one organization to another. The main attributes of an organization, its size and the types of activities it engages in, provide a benchmark for the base level of risk of enterprises of that type. There are many individual characteristics, however, that make a difference to an organization and determine how far above or below it is relative to the average risk rate of its peer group.

1.5.4 Risk of Cyber Catastrophes

In addition to the potential for a severe loss to an individual organization, there is the potential for multiple organizations to be impacted in a single event, which we have termed a cyber catastrophe. The likelihood of cyber catastrophes is an important factor in determining how much effort we, as a society, should put into reducing cyber risk. The risk of a catastrophe occurring is relatively low, but the potential impact could be very severe on our economy, living standards, and way of life. It similarly ranges in a

continuum of severity, from events like *WannaCry* and *NotPetya* that cost billions of dollars through to potential scenarios where cyber attacks could cost the economy trillions of dollars and destabilize our way of life. We consider these as risk curves too, with the severity of events ranked against how probable we think they might be, illustrated in Figure 1.2.

1.6 HOW MUCH DOES CYBER RISK COST OUR SOCIETY?

In this book, we argue that the costs to our economy and disruption to our way of life being posed by cyber attacks are unacceptable, and that they can be reduced and managed to acceptable levels with collective action, individual responsibility, and appropriate resourcing. Cyber risk is a relatively new risk, and is different from the types of risks that society has faced, and dealt with, in the past.

To know how to manage it, we first need to know how much of a problem it is. Measuring a problem as objectively as possible allows us to make rational decisions about protection and resources.

1.6.1 Collecting Information on Cyber Loss Incidents

It is difficult to estimate exactly how much cyber loss incidents cost our society. Some of the losses, particularly those suffered by private companies, are kept confidential. However, many are reported and are on the public record. Any data breaches that compromise personal information are now required to be officially notified and publicized. Incidents that affect shareholders or have wider implications usually find their way into media reports. Larger losses tend to become public. In addition, insured companies claim cyber losses from their insurers, and the authors have worked with insurance companies that have shared their confidential claims statistics. So we believe we have a fairly good representation of the level at which cyber activity is occurring, and can be relatively sure that we have a fairly complete record of the largest events that happen.

For this book we are grateful to Risk Management Solutions, Inc., for the use of its Cyber Loss Experience Database, which is one of the most comprehensive compilations existing; it has identified some 60,000 cyber loss incidences in organizations worldwide from 2007 to 2018, and records hundreds of new events each month.[44] We compare this with the population of organizations that could potentially suffer a cyber loss of these types, derived from census statistics. We take the average rates and patterns of cyber occurrence seen over the past five years and trend them to estimate the annual cost to the global economy at 2019 values.

1.6.2 Incident Rate in Advanced Economies

This analysis suggests that in the most advanced economies at least 1% of large companies (those with more than 500 employees) suffer a large and disruptive cyber loss once a year on average. There are also many additional cyber loss incidents that occur to smaller and medium-size companies, of lesser magnitude and cost. Very large losses occur much less often than smaller losses, but when they do, they result in destabilization of a business, which can lose revenues over the following months as a result of the event, and with consequences for the company's suppliers and counterparties.

1.6.3 Costs of Cyber Attacks to the US Economy

We estimate that in United States the direct costs of payouts and operational disruption to organizations from cyber attacks is averaging around *$20 billion a year*. A further *$225 billion of lost revenues* is suffered by businesses that are impacted so severely that they suffer consequential business loss. Their trading partners and counterparties suffer as a result, and add a further $270 billion of economic loss. In total we estimate that cyber losses cost over *$500 billion a year to the US economy*, which is around *2.5% of US gross domestic product (GDP)*.

1.6.4 Cyber Risk Levels Across the World

Cyber losses in the United States are mirrored by similar losses around the world. Cyber loss is a unique problem in that it is not geographically bounded. Cyber losses have been recorded in more than 150 countries. The number of losses that occur varies significantly from country to country, but this is rapidly converging as nearly all major economies of the world see their information technology systems and data resources come under attack. The costs of cyber events vary significantly in different jurisdictions. Figure 1.3 shows our mapping of the cyber risk across 200 countries, measured by frequency and severity of loss occurring in these economies.

Cyber risk is still highly concentrated in the most IT-dependent economies. We estimate that 90% of all cyber loss by value currently occurs in 18 countries, which between them contribute around 50% of the world's GDP. Around 60 countries account for 99% of cyber loss.

1.6.5 Global Costs of Cyber Attacks

Taking the loss incidence rates across the affected countries, and taking the costs of different types and severities of cyber loss in those jurisdictions, we

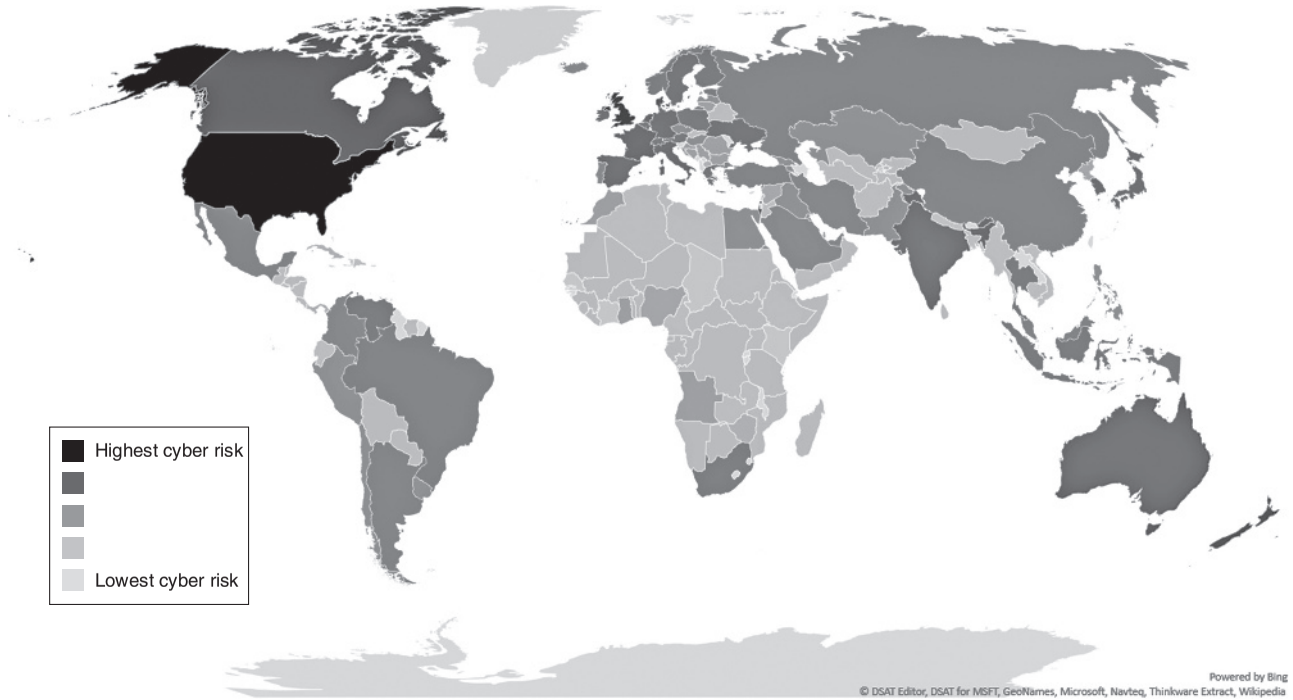

FIGURE 1.3 Cyber catastrophes, their potential impacts, and their estimated likelihoods.

estimate that for organizations across the world, the total direct costs of payouts and operational disruption from cyber attacks each year *exceeds $65 billion*. A further *$725 billion is lost in revenues* by enterprises that are impacted so severely that they suffer a significant level of consequential business loss. This affects their trading partners and counterparties, who also suffer as a result, and this adds a further $820 billion of loss to the economy. In total we estimate that cyber losses cost *over $1.5 trillion a year to the global economy*, just under 2% of the global world product.

1.6.6 Trends of Future Cyber Risk

The estimates here are based on the current levels of cyber activity. These levels of cyber activity are increasing almost everywhere in the world. In addition to the absolute number of cyber attacks increasing, the average size of cyber loss is increasing: a greater proportion of cyber incidents are large losses, possibly as a result of the increasing professionalization of the cyber hacking community. It is likely that cyber risk in on the increase for the foreseeable future.

1.6.7 Risk of Future Cyber Catastrophes

As we have described, the current run rate of losses being experienced from cyber attacks is only part of the risk landscape from cyber threats. Any analysis of the threat of cyber events needs to include the potential for large catastrophic losses to occur that would have major impacts on the economy and on society in general. We cannot assess the likelihood of these occurring with any certainty, but we can make reasonably objective judgments on some order of magnitude of likelihood, based on the rarity of other types of economic shocks and the difficulties of enabling cyber attacks on this scale. Figure 1.2 shows the magnitude of potential economic consequences of cyber catastrophes discussed in Sections 1.1.2 and 1.1.3, with our assessment of the odds of an event as severe as this one occurring within the next year, in any of the advanced markets in the digital economy. We include uncertainty around our estimates. Any analysis of the cost of cyber risk to the economy should include an allowance for the potential for these low-likelihood events with severe consequences. If our economy had to put away funds each year to save up for the costs of these future catastrophes, we would need to put aside around an additional $70 billion to $100 billion each year as catastrophe loading on the economic costs of cyber risk.

1.6.8 Working Together to Solve Cyber Risk

Cyber risk presents a clear and present danger to the functioning of our society and the well-being of our economy. The prosperity that information technology has played such a role in creating for the mainstream populations of the developed economies is now under threat. Cyber risk is not just eroding a steady tax of around 2% on our economic output; it also holds the danger of cascading into massive economic shocks of potentially trillions of dollars.

Solving this risk will not be easy. There is no magic bullet to making cyber risk go away. Individual organizations can install expensive security systems to protect themselves, but this does not stop the threat from raging outside their firewalls, seeking any weakness to attack. No individual organization can solve cyber risk on its own. There are many different stakeholders that need to work together to reduce the drivers, motivations, weaknesses, reward systems, and methods of doing business to change the pattern of risk.

Cyber risk is an unprecedented threat. It will need radically new approaches to solving this risk. This book proposes that we need to take a fresh view at cyber risk, and not be afraid of challenging orthodox approaches.

In the coming chapters we explain cyber risk.

Chapter 2, 'Preparing for Cyber Attacks', gives an overview and examples of the five most costly and significant causes of cyber loss, and how the risk of each of them can be measured and assessed. This chapter includes a short management exercise to prepare your organization for the possibility of experiencing these kinds of loss and to take action to reduce their risk.

Chapter 3, 'Cyber Enters the Physical World,' describes cyber risk to industrial control systems and devices that control our physical world. It outlines the growth of the internet of things (IoT) and how these risks can be managed, both by the manufacturers of the devices and by the users of them in systems.

Chapter 4, 'Ghosts in the Code', covers the issues of vulnerabilities in software, and how these are exploited by threat actors. It describes ways to quantify vulnerabilities, and methods to increase the motivations to reduce the frequency of their occurrence and so reduce cyber risk.

Chapter 5, 'Know Your Enemy', describes the seven generic categories of threat actor that are the key malicious perpetrators of cyber attacks, and describes their different motivations, capabilities, and techniques. It outlines 'hackonomics', the representation of cyber risk in terms of the business

models of different actors and how to consider the threat from the point of view of the risks and the rewards of the perpetrators.

Chapter 6, 'Measuring the Cyber Threat', provides a structure for analyzing the frequency and severity of cyber attacks, and how past examples can be used to explore the counterfactuals of how major cyber events could have turned out differently, and what they tell us about future risk.

Chapter 7, 'Rules, Regulations, and Law Enforcement', covers the rules and regulations that govern the incentives and penalties for organizations managing cyber risk, the complex legal environment, and the law enforcement processes that are trying to combat cyber risk.

Chapter 8, 'The Cyber Resilient Organization', provides an overview of strategies that organizations can use to manage their cyber risk, the levels of investment being made by typical companies, and techniques for optimizing the resilience of an organization.

Chapter 9, 'Cyber Insurance', describes the growing market for cyber insurance, what protection it provides, and the costs and benefits of different aspects of coverage. It describes the challenges for insurance companies managing portfolios of cyber risk and discusses what it will take for the market to meet the demands for risk transfer from the corporate sector.

Chapter 10, 'Security Economics and Strategies', considers the issues of prioritizing cyber security measures in an organization, and measuring the costs and benefits of different tools and processes. It describes the roles of information security officers and risk management at different levels within the organization. It outlines the issues for society in creating incentives for bug discovery and the game theory principles for managing the constant war between attackers and defenders.

Chapter 11, 'Ten Cyber Problems', articulates some of the key issues that currently face security professionals, policy makers, regulators, and the risk managers of organizations in reducing cyber risk in the future.

Chapter 12, 'Cyber Future', considers how the future of cyber risk could evolve, contrasting a pessimistic future where failure to protect the growing digital economy causes financial dysfunction against an optimistic future where cyber risk is minimized and results in beneficial economic growth. We describe key themes for the future, and make 10 recommendations for solving cyber risk.

This book provides a broad overview of cyber risk – its characteristics, its causes, and its potential impact on different enterprises and business activities. We discuss how best to mitigate and protect yourself and your organization from the threat of cyber risk.

And we propose how we can collectively work together to solve cyber risk.

ENDNOTES

1. Security Week (2014).
2. McAfee (2014).
3. Shu et al. (2017).
4. McAfee (2014).
5. Shu et al. (2017).
6. Krebs (2014).
7. Perlroth (2014).
8. Target (2013).
9. Griswold (2015).
10. Griswold (2015).
11. *Forbes* (2014).
12. Cisco (2017). Survey of 3,000 security personnel.
13. Ponemon Institute (2017b).
14. Cisco (2017). Survey of 3,000 security personnel.
15. Yahoo's share price dropped 6.5% after it announced the largest-ever data breach of a billion personal records in December 2016. Sherman, Moritz, and Womack (2016).
16. Ponemon Institute (2017b); HelpNetSecurity (2017); Seals (2017).
17. Equifax, a consumer credit rating organization, had its outlook lowered to negative by Standard & Poor's as a result of its data breach in September 2017. Cherney (2017).
18. Nayana, an internet service provider in South Korea, declared bankruptcy after being hit by *Erebus* ransomware that froze its operations in June 2017. BBC (June 2017).
19. Nortel, a Canadian telecommunications company, filed for bankruptcy in January 2009. Analysts cite cyber theft of its IP among reasons for Nortel being outcompeted in the market by Chinese competitors. Reference GW.
20. Equifax faced a class action lawsuit for up to $70 billion brought by law companies Olsen Daines PC and Geragos & Geragos as a result of its data breach in September 2017, at a time when its valuation was $17 billion. Mosendz (2017).
21. Yahoo's acquisition by Verizon was significantly renegotiated after Yahoo's admission of large-scale data breach incidents, taking the original valuation of $4.8 billion down by $300 million. *Financial Times* (2017).
22. CCRS (2014a).
23. We use the definitions of the US Bureau of the Census in categorizing companies by size in terms of their numbers of employees.
24. Reinsurance (2018).
25. Reinsurance News (2017).
26. AIG (2016).
27. *Leakomania* scenario in RMS (2016).
28. *Extortion Spree*, RMS (2016).
29. *Mass DDoS*, RMS (2016).

30. Cloud Compromise, RMS (2016).
31. ICS Attacks, RMS (2017).
32. E-ISAC (2016).
33. *Erebos* ('Business Blackout') scenario, CCRS and Lloyd's (2015).
34. UK Critical Infrastructure Cyber Catastrophe Scenario, CCRS (2016b).
35. *Global Banking & Finance Review* (2017); Lannin (2017); Gurdgiev (2017).
36. World Economic Forum (2016).
37. Reinhart and Rogoff (2011).
38. Taylor (2010).
39. *Sybil Logic Bomb* scenario, in Ruffle et al. (2014).
40. d'Ancona (2017).
41. *The Times* (2017).
42. Reuters Staff (2016).
43. *China-Japan Geopolitical Conflict* scenario, in CCRS (2014).
44. Cyber Loss Experience Database maintained by Risk Management Solutions, Inc., made available to the authors for this publication.