Chapter 7

Fighting Cybersecurity Threats to the Growing Economy

Information technology creates enormous value for the U.S. economy. However, it also exposes U.S. firms, the government sector, and private individuals to new risks that originate and are often effectuated entirely in cyberspace. Due to the difficulty of identifying and punishing malicious actors, and the ever-greater interconnectedness stemming from the intensified use of the Internet, malicious cyber activity is becoming more and more widespread. Malicious actors range from lone individuals to highly sophisticated nation-states, and they pose a potential threat to all Americans using any information and communications technologies.

Malicious cyber activity imposes considerable costs on the U.S. economy. Some costs are more immediate and include the value of sensitive information and intellectual property stolen by hackers, as well as the loss of revenues, data, and equipment due to disruptive cyberattacks and data breaches. Other costs are longer term, such as the slow rate of adoption of new, productivity-boosting information technologies and the underinvestment in research and development stemming from poor protection against cyber theft. The ongoing costs could escalate considerably in the event of an attack with large-scale consequences—for example, an attack on critical infrastructure sectors that are crucial for the smooth functioning of the U.S. economy.

Cybersecurity is a common good. A firm with weak cybersecurity imposes negative externalities on its customers, employees, and other firms tied to it through partnerships and supply chain relations. In the presence of externalities, firms would rationally underinvest in cybersecurity relative to the socially optimal

level. Therefore, it often falls to regulators to devise a series of penalties and incentives to increase the level of investment to the desired level.

The marketplace is responding to the growing level of cyber threats. Firms are increasingly outsourcing cyber protection functions to the blossoming cybersecurity sector. The emergence of the cyber insurance market helps firms share the risk of cybersecurity compromises. However, these positive developments are hampered by firms' reluctance to share information on past malicious cyber activity directed at them, along with the cyber threats they currently face. This resistance stems from a variety of concerns, such as the fact that investors will respond negatively, causing the stock price to plunge, that the firm will suffer reputational damage and be exposed to lawsuits and regulatory actions, or that the revelation of potential vulnerabilities could lead to additional cybersecurity exposure. Despite the regulatory requirement that material cybersecurity events be reported by publicly traded firms, there is a general agreement that underreporting is pervasive. As a result of this underreporting, the frequencies and costs of various types of malicious cyber activity directed at firms are largely unknown, and this lack of information hampers the ability of all actors to respond effectively and immediately.

In addition, the scarcity of information may be slowing down the development of the cyber insurance market. Further, the use of common technologies among otherwise unrelated firms may impede the development of the cyber insurance market. Common vulnerabilities in these technologies cause cybersecurity risks to be correlated across firms in complicated and little-understood patterns, which makes it difficult for insurance companies to construct properly diversified portfolios of insured firms.

Continued cooperation between the public and private sectors is the key to effectively managing cybersecurity risks. The ongoing efforts by the private sector involve making information technology more secure, providing timely defenses to new threats, and further developing platforms for anonymous information sharing on cybersecurity threats. The government is likewise

important in incentivizing cyber protection—for example, by disseminating new cybersecurity standards, sharing best practices, conducting basic research on cybersecurity, protecting critical infrastructures, preparing future employees for the cybersecurity workforce, and enforcing the rule of law in cyberspace.

This chapter examines the substantial economic costs that malicious cyber activity directed at firms imposes on the U.S. economy. As the U.S. economy relies more and more on information technology (IT) and greater interconnectedness, cybersecurity threats pose an increasing challenge. A malicious cyber activity is defined as an activity, other than one authorized by or in accordance with U.S. law, that seeks to compromise or impair the confidentiality, integrity, or availability of computers, information or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or the information resident thereon.

The theft and destruction of private property are not a new problem in economics. Economists have long understood that the effective enforcement of property rights, for both IP and physical property, underlies economic growth by encouraging investment in physical assets, in research and development, and in putting these assets to productive uses. A law enforcement system that efficiently identifies and punishes criminals, and also actively patrols against criminal activity, reduces crime. Law enforcement actions to disrupt and deter cyber-enabled crime are important components of cybersecurity. Law enforcement has deployed massive resources towards combatting cybercrime, including an entire division of the Federal Bureau of Investigation (FBI) and hundreds of trained Federal prosecutors. However, cybercrimes present particular challenges for law enforcement. The identification of cybercriminals is difficult, because the Internet presents opportunities for user anonymity.

Moreover, the proliferation and sharing of malicious computer code intended to damage or destroy computer systems—malware—makes it difficult to tie particular malware to particular people. Sophisticated actors are able to obfuscate origin and pathways for malicious activities. Even when criminals are identified, punishing them is often difficult because cybercriminals often reside in countries with unfriendly political regimes. In fact, malicious cyber activities are sometimes authorized by such unfriendly regimes. Nonetheless, despite the difficulties, in a significant number of cases cybercriminals have been arrested abroad, including in countries with unfriendly political regimes, to face charges related to cybercrime.

The responsibility for protecting against cybersecurity threats falls largely on individuals and economic entities and not on law enforcement—that

is, unless cyberattacks are directed at critically important infrastructure sectors that are deemed to be crucial for the smooth functioning of the U.S. economy. Firms and private individuals are often outmatched by sophisticated cyber adversaries. Even large firms with substantial resources committed to cybersecurity may be helpless against attacks by sophisticated nation-states.

Further exacerbating the problem, firms may be rationally underinvesting in cybersecurity relative to the socially optimal level because they do not take into account the substantial negative externalities imposed by cyberattacks and data breaches on private individuals and on other firms. For example, as we show later in the chapter, a data breach experienced by Equifax also negatively affected other similar firms, along with Equifax's corporate customers. The firms that own critical infrastructure assets, such as parts of the nation's power grid, may generate pervasive negative spillover effects for the wider economy.

For these and other reasons, cybersecurity risks have increased significantly, and malicious cyber activity imposes substantial costs on the U.S. economy. The Council of Economic Advisers (CEA 2018) estimates that malicious cyber activity cost the U.S. economy between $57 and $109 billion in 2016, which amounts to between 0.31 and 0.58 percent of that year's gross domestic product (GDP). However, this number could pale in comparison with the potential cost that would be incurred by the U.S. economy in the event of a large-scale cyberattack, in which IT is used to disrupt services provided by the government to its citizens and businesses. The additional costs that malicious cyber activity imposes on economic growth are (1) underinvestment in research and development and information assets, due to insufficient protection of property rights; and (2) the slow rate of adoption for new, productivity-boosting IT, for fear that it is insufficiently secure.

One glaring problem that impairs effective cybersecurity is firms' reluctance to share information on cyber threats and exposures. Although the Cybersecurity Information Sharing Act of 2015 made significant progress toward the exchange of threat and vulnerability data between the private and public sectors, firms remain reluctant to increase their exposure to legal and public affairs risks. The lack of information on cyberattacks and data breaches suffered by other firms may cause less sophisticated small firms to conclude that cybersecurity risk is not a pressing problem. In addition, insufficient data on the frequency and costs of cybersecurity events make it difficult for firms to determine the appropriate level of resources to manage the cyber risk. In addition, the lack of data may be stymying the ability of law enforcement and other actors to respond quickly and effectively and may be slowing the development of the cyber insurance market.

Another impediment to a quick development of a competitive market for cyber insurance is insursers' insufficient understanding of their common vulnerabilities to various types of cyber threats. These vulnerabilities could arise

at the level of software, hardware, or cloud computing. Without the ability to properly quantify how cybersecurity risks are correlated across firms, insurers may find it challenging to construct well-diversified portfolios of insured firms.

In response to growing cyber threats, both the public and private sectors are actively working on solutions. The private sector is moving to a more cost-efficient model for cyber protection by outsourcing it to the growing cybersecurity sector. The private sector is also responding by developing IT solutions and by improving information sharing. Also, the cyber insurance market is expanding to meet the growing demand. However, despite this progress, cooperation between the public and private sectors is crucial to effectively respond and to limit the overall risks. As the frequent target of cyberattacks and data breaches, the government can be a valuable contributor to sharing threat information. The government can also create educational programs to ensure that there is a robust pipeline of domestic employees for the cybersecurity workforce. Through a system of penalties and regulations and other levers, the government can incentivize the private sector to increase its investment in cybersecurity to the socially optimal level. Furthermore, the government sector is nearly unmatched in its ability to identify and neutralize cyber threats. Finally, only the government has the authority to punish cybercriminals and thus reduce their incentives to commit future crimes.

The chapter proceeds as follows. The first section gives an overview of cybersecurity risks and cyber threat actors. The second section estimates the costs that cybersecurity events impose on individual firms. The third section discusses the externalities that weak cybersecurity imposes on a firm's customers and on other firms. The fourth section describes how firms' use of the same software, hardware, and cloud computing services makes seemingly unrelated firms vulnerable to the same cyber threat vectors. The fifth section highlights the problems imposed by insufficient data. The sixth section considers the problem of dark cyber debt. The seventh section examines the growing market for cyber insurance. The eighth section describes the costs of malicious cyber activity for the U.S. economy. The ninth section discusses devastating scenarios for cyberattacks and data breaches. The tenth section explains the risks posed by the rise of quantum computing. And the eleventh section describes the ongoing efforts by the private and public sectors to reduce cyber risk.

Malicious Cyber Activities and Cyber Threat Actors

Malicious cyber activities directed at firms can take multiple forms, and they compromise at least one component of what is known as the "CIA triad": confidentiality, integrity, and availability. For example, a distributed denial-of-service (DDoS) attack—which is defined as making an online service

unavailable by overwhelming it with traffic from multiple sources—falls under the "availability" category of the triad because it interferes with the availability of a firm's Web-based services. A theft of funds from a bank customer's account through cyber means violates the integrity of the bank's transactions data. A cyber-enabled theft of the personally identifiable information (PII) of a firm's customers or employees compromises data confidentiality.

We next give the definitions of the terms we use in this chapter. According to the definition proposed by the National Institute of Standards and Technology (NIST), a cybersecurity incident is defined as a violation of "an explicit or implied security policy" (Cichonski et al. 2012). In turn, for NIST, cybersecurity incidents include but are not limited to (1) attempts, either failed or successful, to gain unauthorized access to a system or its data; (2) DDoS attacks; and (3) unauthorized changes to system hardware, firmware, or software. We further distinguish between two types of "successful" cybersecurity incidents: a cyberattack and a data breach. As defined by the Director of National Intelligence, a cyberattack intends to "create physical effects or to manipulate, disrupt, or delete data." According to this definition, a cyberattack interferes with the normal functioning of a business. Thus, DDoS attacks, cyber-enabled data and equipment destruction, and data-encryption attacks fall into the category of cyberattacks. In contrast, a data breach may not necessarily interfere with normal business operations, but it involves unauthorized "movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information," according to the Department of Homeland Security (DHS 2017d). (To draw a parallel to the property rights terminology, a cyberattack destroys property or makes it unavailable for use, and a data breach amounts to property theft.) In this chapter, we also refer to cyberattacks and data breaches as "malicious cyber activity," "adverse cyber events," or simply as "cyber events," and we sometimes refer to data breaches as "cyber theft." When a malicious cyber activity is attributed to a criminal group or when it is directed at private individuals, we sometimes also refer to it as "cybercrime."

According to government and industry sources, malicious cyber activity is a growing concern for both the public and private sectors. Between 2013 and 2015, according to the Office of the Director of National Intelligence (DNI), cyber threats were the most important strategic threat facing the United States (DOD 2015a)—they "impose costs on the United States and global economies" and present "risks" for "nearly all information, communication networks, and systems" (DNI 2017). For more on cyber threat actors, see box 7-1.

Attribution of cyber incidents is difficult, but expert analysis of the malicious code and the attack techniques combined with law enforcement and intelligence collection can identify responsible actors. Verizon's Data Breach Investigations Report notes that 75 percent of recent security incidents and breaches were caused by outsiders, while 25 percent were performed by

Box 7-1. Cyber Threat Actors

Cyber threat actors fall into six broad groups, each driven by distinct objectives and motivations (CSO 2017):

Nation-states: The main actors are Russia, China, Iran, and North Korea, according to the DNI (2017). These groups are well funded and often engage in sophisticated, targeted attacks. Nation-states are typically motivated by political, economic, technical, or military agendas, and they have a range of goals that vary at different times. Nation-states frequently engage in industrial espionage. If they have funding needs, they may conduct ransom attacks and electronic thefts of funds. Nation-states frequently target PII in order to spy on certain individuals. Furthermore, nation-states may engage in business destruction involving one or more firms, potentially as a retaliation against sanctions or other actions taken by the international community, or as an act of war (based on interviews with cybersecurity experts). Cybersecurity experts like to say that in an act of war or retaliation, the first moves will be made in cyberspace. A growing consensus indicates that cyberspace is already being used by nation-states for retaliation against policies/measures, such as sanctions, imposed on them by individual nations or the international community.

Corporate competitors: These are firms that seek illicit access to proprietary IP, including financial, strategic, and workforce-related information on their competitors; many such corporate actors are backed by nation-states.

Hacktivists: These are generally private individuals or groups around the globe who have a political agenda and seek to carry out high-profile attacks. These attacks help hacktivists distribute propaganda or to cause damage to opposition organizations for ideological reasons.

Organized criminal groups: These are criminal collectives that engage in targeted attacks motivated by profit seeking. These groups collect profits by selling stolen PII on the dark web and by collecting ransom payments from both public and private entities by means of disruptive attacks.

Opportunists: These are usually amateur hackers driven by a desire for notoriety. Opportunists typically attack organizations using widely available codes and techniques, and thus usually represent the least advanced form of adversaries.

Company insiders: These are typically disgruntled employees or ex-employees looking for revenge or financial gain. Insiders can be especially dangerous when working in tandem with external actors, allowing these external actors to easily bypass even the most robust defenses.

internal actors (Verizon 2017). Overall, 18 percent of threat actors were state-affiliated groups, and 51 percent involved organized criminal groups. The DNI (2017) notes that Russia, China, Iran, and North Korea, along with terrorists and criminals, are frequent cyber threat actors.

A PricewaterhouseCoopers (PwC 2014) report—based on a survey of more than 9,700 C-level executives, vice presidents, other administrators, and directors of IT and security practices, with 35 percent of the surveyed firms based in the North America—states that malicious cyber activities by nation-states are the fastest-growing category of malicious cybersecurity incidents. Actors who are attacking on behalf of nation-states are among the most technically skilled actors, and attacks by nation-states often go unnoticed by firms. Although, historically, nation-states have sought to steal IP, sensitive financial plans, and strategic information, nation-states are becoming increasingly motivated by retaliation goals, and thus are engaging in data and equipment destruction, and in interrupting business (FBI 2014). The most recent publicly confirmed attack by a nation-state was a destructive WannaCry malware attack initiated by North Korea that is estimated to have cost the world economy billions of dollars (Bossert 2017).

A cyber adversary can utilize numerous attack vectors simultaneously. The backdoors that were previously established may be used to concurrently attack the compromised firms for the purpose of simultaneous business destruction.

Ultimately, any organization is fair game for cyber threat actors, though at different times a different set of firms may face higher risks. For example, corporate competitors typically target firms in their industry. So-called hacktivists, motivated by ideological considerations, may pile on to attack a different set of organizations at different times, typically because these organizations have offended hacktivists' worldviews. We have conducted interviews with a number of cybersecurity experts and, anecdotally, news organizations are among hacktivists' frequent victims. When a nation-state faces sanctions targeting a certain industry, the nation-state may use cyber-enabled means to target firms in that same industry in the country or countries that imposed the sanctions. That said, any firm is a potential target, independent of its age, size, sector, location, or employee composition.

At this time, there is no common taxonomy for categorizing malicious cyber activities. Some cybersecurity experts believe that it is helpful to focus on the motive and associated threat actors. For example, Verizon's 2017 "Data Breach Investigations Report" uses three broad classifications that encompass both motive and threat actor categories: (1) FIG (fun, ideology, grudge, or activist group threat actors); (2) ESP (espionage motive, or state-affiliated or nation-state actors); and (3) FIN (financial motivation, or organized criminal group, actors). A former special adviser on cybersecurity to the White House, Richard Clarke, used a slightly different set of classifications: (1) hacktivists; (2) cybercriminals; (3) cyber espionage; and (4) large-scale cyberattacks (Verizon 2017; Hughes et al. 2017). As the field of cybersecurity evolves, the Council of Economic Advisers believes that it will be helpful to develop a common lexicon with which to delineate categories of malicious cyber activity.

The Costs of Adverse Cyber Events Incurred by Firms

A survey of firms located in the United States and in other countries, representing different industries and firm sizes, conducted by Ponemon (2017a) revealed that a typical firm experiences 130 security breaches each year.[1] If not addressed, a security breach may evolve into materially damaging cyber event. Because many firms employ security procedures that help detect and neutralize cyber threats (e.g., by employing tools for detecting and containing security breaches as well as procedures for quick recovery), security breaches do not necessarily result in a material impact such as a business disruption, data theft, or data or property destruction. When a firm does fall victim to an exploit or other attack, it may face a range of loss categories, some of which are easy to observe and quantify, and some of which are not.

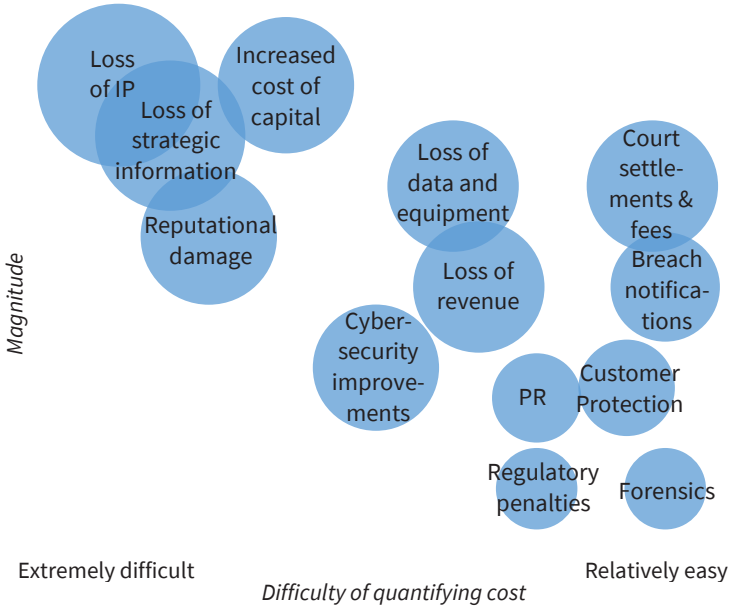
Figure 7-1 illustrates the costs associated with materially damaging cybersecurity events. These costs vary across firms and categories of cyberattacks or data breaches. Depending on the nature of their operations, firms are generally exposed to different cyber threats. Consumer-oriented firms with a prominent Web presence, such as online retailers, are more likely to be targeted for a DDoS attack, while firms engaging in research and development, such as high-technology companies, are more likely targeted for IP theft.

To provide context for this figure, consider potential costs of a DDoS attack. A DDoS attack interferes with a firm's online operations, causing a loss of sales during the period of disruption. Some of the firm's customers may permanently switch to a competing firm due to their inability to access online services, imposing additional costs in the form of the firm's lost future revenue. Furthermore, a high-visibility attack may tarnish the firm's brand name, reducing its future revenues and business opportunities.

The costs incurred by a firm in the wake of IP theft are somewhat different. As the result of IP theft, the firm no longer has a monopoly on its proprietary findings because the stolen IP may now potentially be held and utilized by a competing firm. If the firm discovers that its IP has been stolen (and there is no guarantee of such discovery), attempting to identify the perpetrator or obtain relief via legal process could result in significant costs without being successful, especially if the IP was stolen by a foreign actor. Hence, expected future revenues of the firm could decline. The cost of capital is likely to increase because investors will conclude that the firm's IP is both sought-after and not sufficiently protected. In addition, an adverse cyber event typically triggers a

[1] In the absence of a centralized data set on cyberattacks and data breaches, many statistics reported in this chapter come from surveys. The usual limitations of survey data apply, such as that the set of reporting firms may not be representative, or the reported results may not be accurate. Due to the reluctance of firms to report negative information, discussed later in the chapter, the statistics may be biased down due to underreporting.

Figure 7-1. Cost Components of an Adverse Cyber Event



Sources: McKinsey; CEA calculations.

range of immediate and relatively easily observable costs, such as expenditures on forensics, cybersecurity improvements, data restoration, legal fees, and the like.

Using survey data from 254 companies, Ponemon (2017a) computes estimates of what share of the total immediately observable, cyber-driven loss each individual cost component represents: (1) information loss, 43 percent; (2) business disruption, 33 percent; (3) revenue losses, 21 percent; and (4) equipment damages, 3 percent. Moreover, the case studies provided in this chapter's boxes illustrate how firms, by limiting their consideration to only immediately observable losses when evaluating the impact of malicious cyber activity, may drastically underestimate the total losses they could suffer.

Estimating the Costs of Adverse Cyber Events for Firms

The least subjective method for estimating the impact of a cybersecurity events on a publicly traded firm is to quantify its stock price's reaction to the news of such events. For a publicly traded firm, its market value reflects the sum of (1) the value of its current assets and (2) the present discounted value of all future cash flows that the firm is expected to earn over its life span. In efficient capital markets, the market value will adjust quickly to reflect a new valuation following any news that affects the firm value. We use an event study methodology to calculate how market prices react to news of cyberattack or a data breach to

quantify the impact the exposure on a firm's value. All the costs shown in figure 7-1 are automatically accounted for in this calculation, reflecting the market's view of how the sum of these costs lowers the firm's value.

In this analysis, we rely on the newsfeed from Thomson Reuters for public news of cyberattacks and data breaches suffered by specific firms. The main readerships of the Thomson Reuters newsfeed are institutional traders and investors, who rely on it for breaking news on firms and markets. From this newsfeed, we separate out news of cyberattacks and data breaches suffered by individual firms. We identify news of such events by searching news headlines for key words such as "cyberattacks," "hacking," "data breach," and the like, including spelling and syntactic variations of these keywords. To isolate the impact of the events on stock prices, we remove announcements of cyberattacks and data breaches that fall within seven days of a quarterly earnings announcement. Moreover, we exclude news stories concerning cybersecurity firms, isolating only those firms that have been victims of malicious cyber activity. Because malicious cyber activity is a relatively new phenomenon, we start our analysis in January 2000 and run it through the last month of the available data, January 2017.

To estimate the impact of an adverse cyber event on a firm's value, we estimate the reaction of its stock price over the event window that begins on the day that the adverse cyber event was publicly disclosed in the news and ends seven days later. We employ the methodology used in prior event studies (e.g., Neuhierl, Scherbina, and Schlusche 2012). We consider two widely used models, the market model and the Capital Asset Pricing Model, to estimate baseline returns. Both models produce similar results, and we report only results based on the market model. In the market model, the market return is subtracted from the stock return in order to calculate the abnormal stock return on each event day. These values are then summed over the event window to calculate a cumulative abnormal return (CAR). Moreover, because Thomson-Reuters frequently issues closely spaced updates on prior adverse cyber events, we require that each subsequent news articles be at least seven days removed from the previous news—which effectively removes updates on a previously reported news item.

Our final data set contains news of 290 adverse cyber events committed against 186 unique firms. Because institutional customers of newsfeeds typically trade large and liquid stocks, newsfeeds disproportionately cover large firms. As a result, the firms in our data set have relatively high market capitalizations. The market capitalization of a median firm in our data set is $12 billion, which is as large as that of a firm belonging to the ninth-largest size decile of all firms trading on the New York Stock Exchange (NYSE) (and firms trading on the NYSE tend to be larger than firms trading on other exchanges). The market capitalization of an average firm in our sample is even higher than that of a median firm—equal to $65 billion.

We find that the stock price reaction to the news of an adverse cyber event is significantly negative. Firms on average lost about 0.8 percent of their market value in the seven days following news of an adverse cyber event, with the corresponding *t* statistic of –2.35. This *t* statistic is statistically significant and makes a researcher highly confident that the underlying stock price's reaction to the news of an event is negative. (Also, this *t* statistic implies that there is less than a 2 percent chance that a researcher would have obtained this particular negative estimate if stock price reactions to the cybersecurity event were distributed around the mean of zero.) We estimate that, on average, the firms in our sample lost $498 million per adverse cyber event. The distribution of losses is highly right-skewed. When we trim the sample of estimated losses at 1 percent on each side of the distribution, the average loss declines to $338 million per event. The median loss per event is substantially smaller, and equals $15 million. By comparison, PwC (2014) reports that in 2014, the average cost attributed to cybersecurity incidents was $2.7 million. Another industry source, Ponemon (2017a), uses a survey sample of 254 relatively large companies (hence, the size of the firms is closer to that in our sample) and estimates that an adverse cyber events cost these firms $21 million per event, on average.

The number of cyberattacks and data breaches reported by Thomson Reuters has been increasing over the years, likely for these reasons: (1) More firms experienced adverse cybersecurity events in later years, (2) investors started to pay more attention to and demand reports on such events, and (3) more advanced technology has improved breach detection and allowed for a better deflection of DDoS attacks. Of the 290 events in our sample, only 131 were reported in the 13 years before 2014, and 159 were reported after 2014.

Previous studies and reports speculated that the market was not entirely rational, or perhaps was too slow when evaluating the costs of adverse cyber events because of the lack of data on past events (e.g., Kvochko and Pant 2015). Table 7-1 presents CARs to the news of adverse cyber events, by sample period.

The table shows that though in the earlier subperiod, the average stock price reaction is negative, the corresponding *t* statistic indicates that it is statistically indistinguishable from zero. In the second subperiod, the stock price reaction is significantly negative; there is less than a 1 percent chance that researchers would have obtained the negative CAR estimate purely because of noise in the data if stock prices did not reliably drop in response to news of a cyberattack or a data breach. These results suggest that the market has gained a better understanding of the costs of adverse cyber events and thus has started reacting to news of such events more quickly.

Our study improves on earlier ones with respect to the costs of adverse cyber events, in that it both uses a longer and more complete data set of such events and in that it estimates the costs from stock price reactions. We obtain markedly more negative estimates of the impact of adverse cyber events on

Table 7-1. Cumulative Abnormal Returns (CARs) Following News of an Adverse Cyber Event, 2000–2017

Sample period	Number of events	CAR (%)	*t* statistic
2000–2013	131	–0.53	–0.8
2014– Jan. 2017	159	– 1.01	–3.42

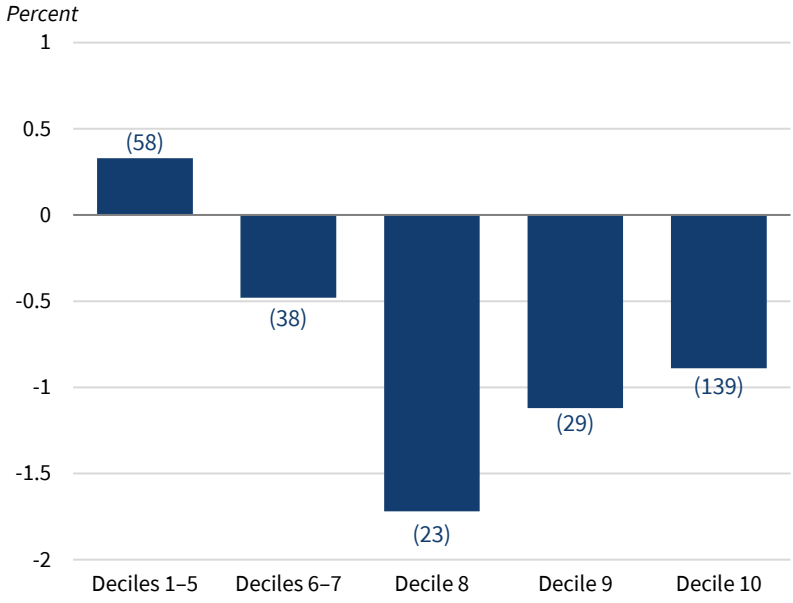
Sources: Thomson Reuters; CEA calculations.

firm values than earlier studies (e.g., Hilary, Segal, and Zhang 2016; Kvochko and Pant 2015; Romanosky 2016), for four reasons. First, our sample includes a wider variety of adverse cyber events, whereas earlier studies (e.g., Hilary, Segal, and Zhang 2016) mainly used reported data breaches that involved PII. Second, our estimations analyze market reactions to the news of adverse cyber events, whereas some of the earlier studies consider only a subset of measurable and observable costs that would be covered by cyber insurance. Third, our sample extends to a more recent period, during which stock price reactions to cyber news became more immediate. Fourth, our sample of cyber events is newsworthy enough to warrant a report in the Thomson Reuters news feed, and, therefore, may be worse in terms of the damage caused than cyberattacks and data breaches that are not covered in the business press.

We next analyze whether firms of different sizes react differently to the news of cyber events. If a cyberattack or a data breach causes the same dollar damage for two firms of different sizes, the event would have a smaller impact on a larger firm than on a smaller firm. For example—as illustrated by the case of SolarWorld, which is discussed later in the chapter—smaller firms, and especially those with few product lines, can easily go out of business if they are attacked or breached. (Note that going out of business translates into a –100 percent return on equity.) We form firm size bins based on the NYSE size deciles, but because our sample contains very few small firms, we further aggregate several size deciles into a single bin for smaller firms. The results, illustrated in figure 7-2, show a U-shaped relation between firm size and the stock price reaction to the news.

Specifically, figure 7-2 shows that firms in the 8th NYSE size decile experience the lowest CARs in response to the news of adverse cyber events, equal to –1.72 percent. Firms in the 9th and 10th NYSE size deciles have CARs equal to –1.12 and –0.89 percent, respectively. We believe that the CARs associated with such cyber events experienced by smaller firms, those in deciles 1 through 7, may be less negative, for three reasons. First, the reported events may have been less devastating. Second, the costs may have been largely covered by cyber insurance. And third, perhaps most important, stockholders of smaller firms are typically retail investors rather than more sophisticated institutions, so they may take longer than seven days to react to news about cyber events

Figure 7-2. Cumulative Abnormal Return by Firm Size



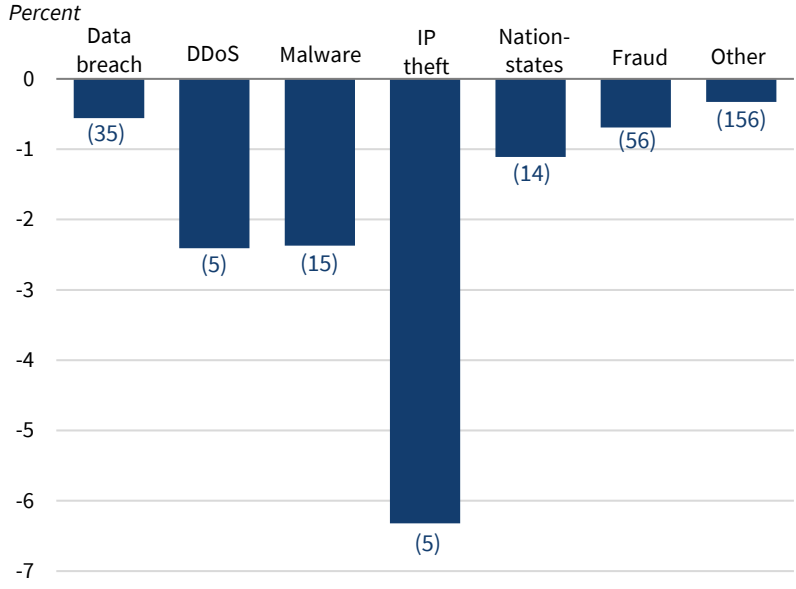
Sources: Thomson Reuters; CEA calculations.
Note: Number of observations is in parentheses.

involving firms whose stocks they hold. Hence, the full price impact of the adverse cybersecurity events will not show up within the seven-day time frame.

Despite the small sample size, we further subdivide the adverse cybersecurity events into different categories using key word searches. We attempted to make these categories consistent with the cybersecurity industry classifications, but because the news media use varied naming conventions, the resulting categories are somewhat different. For example, some adverse cyber events are only described in the news headline as having been attributed to nation-states with no additional information on the types of events. Hence, we include a category classified simply as "nation-state." All categories of adverse cyber events are made to be mutually exclusive; each incident in our data set may have exactly one classification.

We began by identifying data breaches that may involve the theft of PII. This category of adverse cyber events received the most attention from State regulators, as indicated by various State laws that mandate firms to disclose instances of PII theft. (As of April 2017, 48 States, the District of Columbia, Puerto Rico, Guam, and the Virgin Islands have put in place legislation mandating that government organizations and/or private businesses "notify individuals of security breaches of information involving personally identifiable information" (National Conference of State Legislatures 2017).) We identified

Figure 7-3. Cumulative Abnormal Return by Type of Adverse Cyber Event



Sources: Thompson Reuters; CEA calculations.
Note: Number of observations is in parentheses.

35 adverse cybersecurity events that fall under this classification. From the remaining sample, we identified cyberattacks that were reported to result in the destruction of data or equipment, ultimately finding only one attack of this nature. Using the rest of the sample, we identified the news of DDoS attacks; we found a total of 5 observations in this category.

Next, headlines that mentioned the use of malware, spyware, ransomware, and the like had 15 observations; we classified this category as "malware." Of the remaining news, 5 involved espionage and and/or the theft of IP; we classified this category as "IP theft." Using the remaining observations, we next searched for the mention of "nation-states," and specifically Russia, China, Iran, or North Korea. We were able to identify 14 attacks in this category, and we classified them as "nation-states."[2] Of course, nation-states may also have been involved in the previously classified four categories of adverse cyber events. Finally, we searched for the mention of wire fraud, the type of malicious cyber activity that predominately affects financial firms. This category has the highest number of headlines, 56. The remaining unclassified observations were assigned to the category "other."

Figure 7-3 shows the average seven-day CARs associated with the various categories of cyber events in our sample, with the number of observations per

[2] It is important to note that a reference to nation-state in the news media does not necessarily reflect the attribution made by the U.S. government.

each category reported in parentheses. We show only the categories with at least five observations and, therefore, excluded the category involving destructive attacks because it had only one observation.

Although based on a small sample, the figure shows that the market perceives cyber events involving IP theft to be the most damaging, with the victim firms losing, on average, 6.32 percent of their market value. DDoS attacks are a distant second in terms of the damage caused, with attacked firms losing 2.41 percent of market value due to a DDoS attack. As discussed above, DDoS attacks on those consumer-oriented firms that have a heavy online presence have the potential to cause business disruptions that result in lost customers and reputational damage. Moreover, according to our interviews with cybersecurity experts, while contemporaneously using a DDoS attack to distract cyber protection resources, threat actors often engage in malicious intrusions in the victim firm's network. Malware attacks are a close third in harm caused, with an associated average drop in market value of 2.37 percent. Cybersecurity experts have related to us that a number of malware attacks in our sample had an objective of data destruction rather than ransom, and that this destruction of data could have been extremely damaging for the affected firms.

News of adverse cyber events that mention nation-states in the headline, on average, led to a 1.11 percent drop in market value. "Fraud" events involving monetary theft, which typically targeted financial firms, caused average losses of 0.69 percent of a firm's market value. Events that involved data breaches are relatively less damaging for victim firms, on average causing losses of only 0.56 percent. We believe that the theft of PII data on firms' customers and employees mainly represents an externality, for which firms are not excessively penalized by the market. Finally, the "other" catchall category of cyber events is the least damaging on average, with the typical event resulting in a 0.33 percent drop in a firm's market value.

Although it may be informative to study the longer-run effect of announcements of cyberattacks and data breaches on stock prices, in case stock prices underreact or overreact in the short run,[3] such an analysis would need to be done at the portfolio level (by combing together into a portfolio multiple firms that experienced these adverse cyber events at about the same time) rather than at the individual stock level and would, therefore, require more observations of news of such events than what we have in our data set in order to be

[3] E.g., the academic literature on the post-earnings announcement drift has shown that stock prices tend to underreact to earnings surprises, and the stock price drifts in the direction of the initial reaction for up to several months in the future.

convincing (for a description of this econometric approach, see, e.g., Mitchell and Stafford 2000).[4]

The effect of adverse cyber events on small and medium-sized businesses. Due to the nature of our sample, small and medium-sized firms were excluded from our analysis. However, such events may be more devastating for smaller firms because, for example, for a business that is focused on a single product, IP theft could wipe out the firm's entire livelihood. Similarly, a business disruption that lasts several days could cause customers to permanently abandon a small firm. Finally, the fixed costs of dealing with a breach or attack—such as the cost of cybersecurity improvements and legal fees—would represent a larger fraction of a small firm's operating budget. The 2015 *Year-End Economic Report* of the National Small Business Association (2015) estimated that, based on survey evidence from 884 small-business owners, 42 percent of respondents experienced a breach or an attack. Small and medium-sized businesses are at a high risk of being attacked by ransomware, which renders a firm's files inaccessible until a ransom is paid, along with attacks that exploit weaknesses in email systems in order to trick firms into transferring large sums of money into the perpetrators' bank accounts. According to the survey, an adverse cyber event costs the victim company over $7,000 on average. For small businesses whose business banking accounts were hacked, the average loss was $32,000. For the median company in the same study, in terms of revenues, these numbers represent, respectively, 0.28 percent and 1.28 percent of firm revenue. Although these are fairly low numbers, events are typically underreported, and the firms in the survey likely only quantify immediate and easily observable losses.

According to anecdotal evidence and various industry sources, a nontrivial number of small businesses go bankrupt as a result of a breach or attack. In so-called perfect capital markets, corporate bankruptcies are not costly because the corporate assets are reallocated toward best uses. However, in the real world, corporate bankruptcies are associated with deadweight losses; some ongoing projects will be permanently abandoned, the output of the research and development efforts will be lost, and firm-specific hard assets may be abandoned or sold at deep discounts.

Case studies of various types of cybersecurity incidents. We next examine in greater detail the various categories of cybersecurity events that occur in the United States and abroad. Most of the firms in case studies are not in our sample, either because the events happened outside our sample period

[4] Several recent studies find that stock prices of firms that experienced a cybersecurity incident completely recover in the long run. However, the results of these studies should be interpreted with caution. A number of these studies lack a proper control group of otherwise similar firms that did not experience an event. In other studies, the high longer-run returns may be explained by positive idiosyncratic (firm-specific) news that occurred subsequent to the announcement of the breach or attack. Interestingly, many firms affected by cyber incidents subsequently announce increased investments in cybersecurity. Possibly, the return on this type of investment is very positive. The return on investment in cybersecurity needs to be studied more closely.

or because the firms were either privately held or listed on a foreign stock exchange. These case studies, along with cyberattacks and data breaches experienced by specific firms described in the text, are based entirely on media reports and our own calculations using public sources, not on an investigation by any government agency, and this report should not be taken as an authoritative description of the events, or as an accusation of criminal conduct. These case studies are designed to illustrate that different firms may be targeted for different reasons, and that malicious cyber activity can easily cause substantial material damage to firms.

The first case study is of a PII data breach at Equifax (box 7-2), which illustrates that a breach involving PII data can be devastating for a firm if its business model is predicated on mass collection of PII.

The second case study is an attack by a nation-state on Sony (box 7-3). The Sony case illustrates an attack by a nation-state. It is one of the few cyberattacks or data breaches publicly attributed to a nation-state actor by the U.S. government.

The Sony attack had adverse effects on the relationship between the United States and North Korea, and it influenced U.S. cybersecurity policy. In response to what it called "the Democratic People's Republic of Korea's numerous provocations," the Obama Administration filed sanctions against various individuals and organizations tied to the North Korean military and technology sectors, barring them from access to the U.S. financial system. President Obama also announced additional legislative proposals in response to the attack, highlighting the need for greater cybersecurity information sharing and a modernization of law enforcement's response to malicious cyber activities.

The third case study is on IP theft. According to figure 7-3, IP theft is the costliest type of malicious cyber activity. Moreover, security breaches that enable IP theft via cyber often remain undetected for years, allowing the periodic pilfering of corporate IP. Box 7-4 illustrates that the theft of IP and other sensitive information can have a devastating effect on an IP-centered, narrowly focused firm.[5]

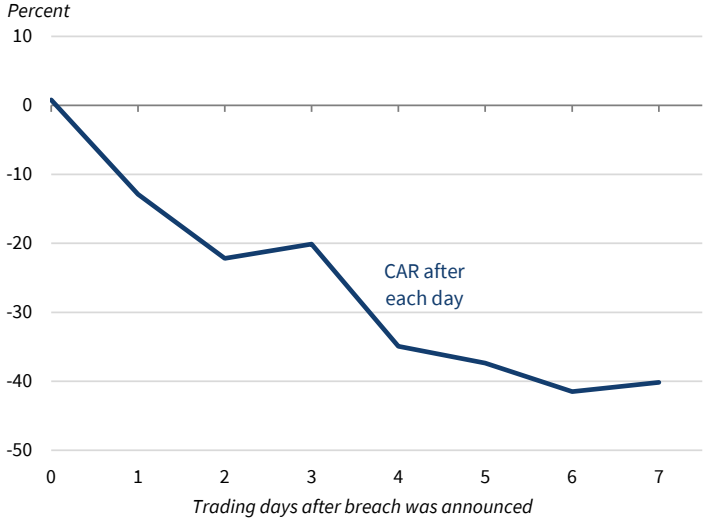
[5] Cyber-enabled IP theft is a subset of the pervasive problem of IP theft that imposes a substantial cost on the U.S. economy. Frequently, IP is stolen by noncyber means. For example, pirating and counterfeiting of IP-protected products typically involves copying an observed design. According to the Commission on the Theft of Intellectual Property (2017), China accounts for 87 percent of counterfeited goods sized coming to the United States. Additionally, trade secrets may be stolen using noncyber means, such as by employee raiding. Finally, the transfer of IP may result from unfair trade practices, and U.S. firms operating in China may be particularly vulnerable to such practices.

Box 7-2. PII Data Breach at Equifax

The September 7, 2017, public announcement that disclosed the magnitude of the data breach experienced by Equifax came after a series of notable events. Equifax first detected the breach that compromised over 140 million personal records (e.g., names, addresses, and Social Security numbers) in July 2017, and it contracted Mandiant, an independent cybersecurity firm, to assist with forensic analysis (Equifax 2017a). Contemporaneously to these investigations, but before the details were publicly disclosed, Equifax executives exercised their stock options and sold shares worth nearly $2 million (Equifax 2017b). Upon finally announcing that it had been the victim of a data breach and sharing the magnitude of the breach, Equifax's share price declined by 13.7 percent over the course of the following trading day. Equifax's executives were later formally investigated for insider trading, and the then-CEO ultimately resigned (Equifax 2017c).

The data breach impelled calls for government action, with multiple Federal agencies launching investigations in the weeks following the breach (Nasdaq 2017). The breach thus put Equifax's entire business model at risk (CNBC 2017). The breach prompted a large downward move in the value of Equifax stock, with share prices falling by as much as 34.9 percent of pre-breach prices (CEA calculations). Cumulative abnormal returns for the seven days after the breach totaled –41 percent, with a *t* statistic of –15.8 (figure 7-i).

Figure 7-i. Equifax's Cumulative Abnormal Returns After Its September 2017 Data Breach Announcement



Sources: Bloomberg; CEA calculations.

The implied volatility of Equifax's one-year option increased by 184 percent, indicating that investors perceive the future of Equifax to be largely uncertain over the next year (CEA calculations). This high perceived uncertainty about Equifax's future will likely negatively affect the firm's ability to raise new capital and make new investments.

Box 7-3. Cyberattacks by a Nation-State: Sony Pictures Entertainment

Sony Pictures Entertainment (SPE) is a U.S. based subsidiary of the Sony Corporation of Japan. SPE's global operations encompass film, television, and digital content production. In 2013, SPE generated $7.77 billion in sales (at end-of-period dollar/yen exchange rates), accounting for 11 percent of the Sony Corporation's total revenue (Sony 2014).

SPE officials and employees, and the general public, first learned of the attack on November 24 (Richwine and Finkle 2014). Hackers identifying themselves as the "Guardians of Peace" claimed to have gained entry to SPE's servers and had stolen over 100 terabytes of confidential information, including employees' Social Security numbers and health records, private emails, and unreleased films such as *Still Alice* and *Annie* (Ignatius 2015). At this point, SPE executives completely shut down computer systems, communicating solely in person or over the telephone. During the following weeks, portions of the stolen SPE data, including personal and sensitive emails between top executives, were repeatedly dumped on public websites and circulated by members of the press.

On December 8, the group posted more confidential SPE data and demanded that the company "stop immediately showing the movie of terrorism which can break the regional peace and cause the War" (Richwine and Finkle 2014). This was widely interpreted as a reference to SPE's *The Interview*, a comedy about a journalist's attempt to assassinate North Korean dictator Kim Jong Un. On December 16, this threat became explicit, when the group threatened 9/11-style consequences for moviegoers attempting to see the film. After the threats against moviegoers, the major theater chains announced that they would not show *The Interview*, and Sony canceled its theatrical release. SPE subsequently announced that *The Interview* would be made available via its online streaming platforms and would be shown in 300 small, independent theaters (Stelter 2014).

Immediately after the attack occurred, Sony officials reached out to the FBI to determine the source of the cyberattack. On December 1, 2014, the FBI released a Flash Alert related to the attack to a limited distribution group (Finkle 2014). In a subsequent report released on December 19, the FBI publicly attributed the attack to North Korean hackers (FBI 2014). According

to the FBI, technical analysis of the data deletion malware used in the attack revealed links to other malware that the FBI had previously attributed to North Korean actors. The attack also used the same tools as previous cyberattacks on South Korean banks and media outlets, which were carried out by North Korea. These findings were supported by a later report from a leading cybersecurity firm, concluding that the attack had the same signatures as previous attacks on South Korean and American targets and thus were unlikely to be the work of hacktivists or a disgruntled employee (Novetta 2016).

Although the share prices increased during the period of the attack, SPE incurred significant costs, including those related to investigation and remediation. Press reporting indicates that the $41 million was damage that SPE may have incurred in March 2015 (Sony 2015), but even one such article notes: "But there are a lot more costs to come. In addition to expenses for investigation of the attack, IT repairs, and lost movie profits, Sony faces litigation blaming it for poor cybersecurity that exposed employees' private information" (Elkind 2015).

Box 7-4. Cyber Theft of IP and Sensitive Corporate Information: SolarWorld

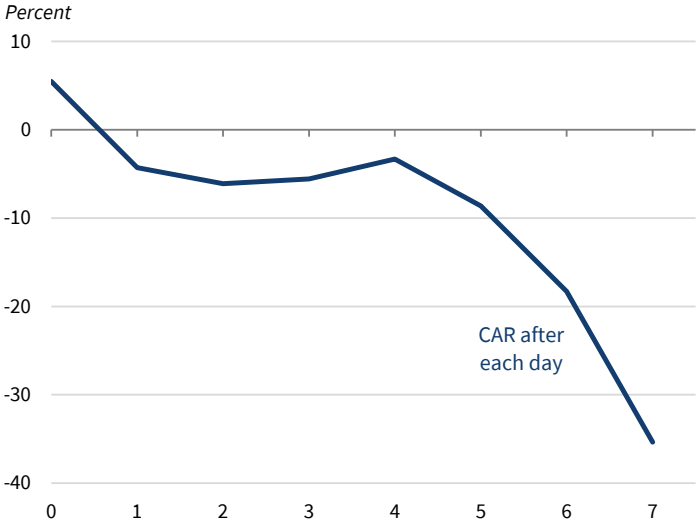
SolarWorld AG is a German company that manufactures and markets products for harvesting solar energy. Between May and September 2012—at about the same time that SolarWorld was an active litigant in trade cases against Chinese solar manufacturers, alleging that they were dumpling products into the U.S. market at prices below fair value—SolarWorld's network was the target of IP theft. In May 2014, Federal prosecutors indicted five Chinese nationals on charges of espionage, trade secret theft, and computer fraud for hacking the networks of six U.S. companies, including U.S. subsidiaries of SolarWorld AG, over a period of eight years (DOJ 2014). In a series of approximately 13 intrusions, thousands of emails and files were stolen from seven executive-level employees. Among the stolen data was information on SolarWorld's financial state, production capabilities, costs, business strategy, and strategy related to the ongoing trade litigation (*United States v. Wang Dong* 2014).

By breaching SolarWorld, Chinese competitors were able to gain access to information that provided them an unfair advantage on multiple fronts (DOJ 2014). A stolen cash flow spreadsheet allows a competitor to know exactly how long SolarWorld would be able to survive a shock. Additionally, production or manufacturing information can be copied without investing time and money into research, and the information on SolarWorld's costs would allow a competing firm to price its products at a rate that would make SolarWorld financially unviable (*United States v. Wang Dong* 2014). The access to the SolarWorld's trade litigation strategy would provide an unfair

advantage to Chinese respondents. SolarWorld has since testified that the cyber theft allowed Chinese manufacturers to use its proprietary research to accelerate their own production timelines, resulting in a long-term loss of competitive advantage and return on investment (USTR 2017). As the result of the cyber theft, which became widely known and reported on in the aftermath of the highly publicized charges, SolarWorld AG (traded on the German DAX) lost 35 percent of its market value (with the corresponding *t* statistic of –1.9) (figure 7-ii; day 0 in the figure is the day on which the charges were announced), which amounted to a loss of €178 million (CEA calculations).

In May 2017, SolarWorld AG filed for insolvency, and SolarWorld America, the American subsidiary, was put up for sale to help cover the parent company's debt obligations (Steitz 2017; SolarWorld 2017).

Figure 7-ii. SolarWorld's Cumulative Abnormal Returns After Its Data Breach Become Publicly Known



Sources: Bloomberg; CEA calculations.

The Distribution of Adverse Cyber Events across Sectors

How are adverse cyber events distributed across sectors? Based on the results of the 2014 survey of 9,700 firms, PwC (2014) reports that nation-states often target critical infrastructure providers and suppliers in order to steal IP and trade secrets as a means to advance their political and economic advantages (we describe the 16 designated critical infrastructure sectors later in the chapter). At the time of the report, cyber incidents that involve nation-states

Table 7-2. Number of Security Incidents and Breaches by Victim Industry and Organization Size, 2016

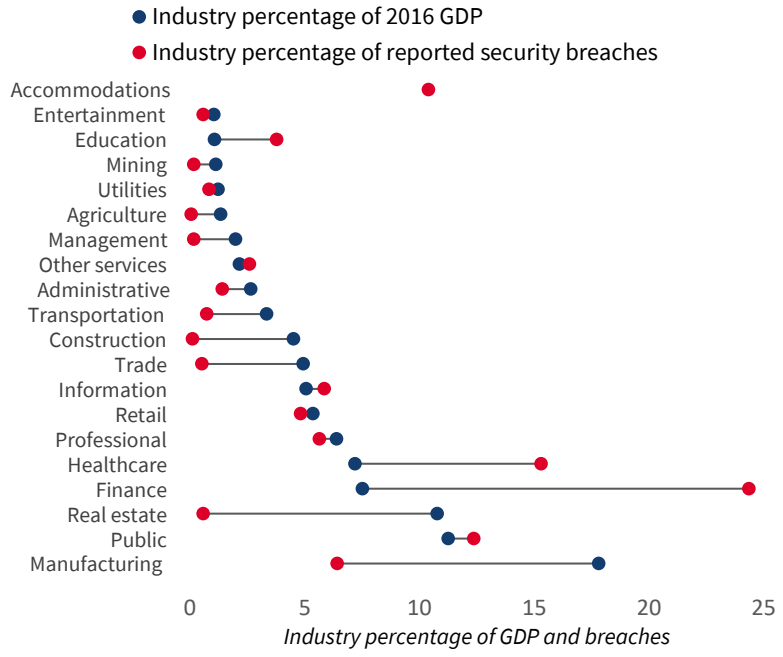
Sector	Incidents				Breaches			
	Total	Small	Large	Unknown	Total	Small	Large	Unknown
Total	42,068	606	22,273	19,189	1,935	433	278	1,224
Accomodation	215	131	17	67	201	128	12	61
Adminstrative	42	6	5	31	27	3	3	21
Agriculture	11	1	1	9	1	0	1	0
Construction	6	3	1	2	2	1	0	1
Education	455	37	41	377	73	15	15	43
Entertainment	5,534	7	3	5,524	11	5	3	3
Finance	998	58	97	843	471	39	30	402
Healthcare	458	92	108	258	296	57	68	171
Information	717	57	44	616	113	42	21	50
Management	8	2	3	3	3	2	1	0
Manufacturing	620	6	24	590	124	3	11	110
Mining	6	1	1	4	3	0	1	2
Other Services	69	22	5	42	50	14	5	31
Professional	3,016	51	21	2,944	109	37	8	64
Public	21,239	46	20,751	442	239	30	59	150
Real Estate	13	2	0	11	11	2	0	9
Retail	326	70	36	220	93	46	14	33
Trade	20	4	10	6	10	3	6	1
Transportation	63	5	11	47	14	3	4	7
Utilities	32	2	5	25	16	1	1	14
Unknown	8,220	3	1,089	7,128	68	2	15	51

Source: Verizon, 2017 Data Breach Investigations Report.

were most frequent in the energy, aerospace and defense, technology, and telecommunication sectors.

According to Verizon (2017), the finance sector, both public and private, saw the most security breaches in 2016, summarized in table 7-2. Manufacturing, government, finance, and healthcare, which made up among the largest shares of U.S. GDP in 2016, also saw the highest shares of security breaches in Verizon's sample. Like NIST, Verizon (2017) defines a security incident as an event that compromises the CIA triad of a corporate asset, while a breach is "an incident that results in the confirmed disclosure—not just the potential exposure—of data to unauthorized authority." Large companies saw the most incidents, while small companies reported the highest number of breaches relative to incidents, suggesting that small companies are not as well equipped to neutralize such security intrusions as large companies. Verizon

Figure 7-4. Distribution of Security Breaches by Industry



Source: Bureau of Economic Analysis; Verizon; CEA calculations.

(2017) defines large companies as those with more than 1,000 employees, and the rest as small companies.

Figure 7-4 plots the share of total cyber breaches and the sector share of the 2016 GDP, in the order of the declining GDP share. The figure shows that finance, healthcare, education, and accommodation suffer a disproportionate number of breaches relative to their contribution to GDP. These sectors are particularly attractive to malicious cyber actors because they possess valuable PII data of their customers.

Externalities from Weak Cybersecurity and Underinvestment in Cyber Protection

In this section, we describe how the presence of externalities creates incentives for private firms to underinvest in cybersecurity relative to the socially optimal level of investment. Cybersecurity is a common good. Thus, weak cybersecurity carries a cost not only to the firm itself but also to the broader economy through the negative externalities imposed on the firm's customers and employees and on its corporate partners. When the PII of a firm's employees and customers is stolen, in the absence of penalties and mandatory customer protections, the burden of the costs falls on customers. A malicious cyber activity directed against a particular firm could also have a negative spillover effect on other

firms connected to the firm through the supply chain, business partnerships, or other firms with similar business models. Because the costs are not borne by the compromised firm, they represent negative externalities. We describe these externalities in detail in the next subsection.

Spillover Effects to Economically Linked Firms

Due to the immense scope of Equifax's data breach and Equifax's centrality in the consumer credit sector of the economy, its data breach caused multiple spillover effects across similar firms and firms tied to it through the supply chain, such as companies that issue credit cards. Scherbina and Schlusche (2015) argue that co-mentions in the news media provide information on economic linkages between firms. By doing news searches of Bloomberg, and by noting firm co-mentions with Equifax over the month preceding the announcement of the breach, we determined the firms that would face the largest spillover effects due to the economic linkages and analyzed the price reactions of these firms to the news of the Equifax data breach.

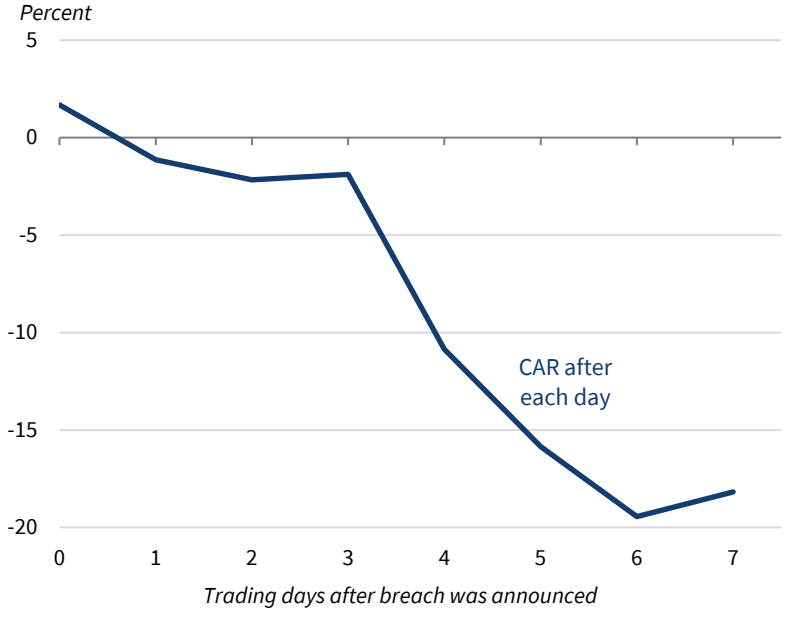
There are at least two companies that have similar business models: TransUnion and Experian. Contemporaneous with the ongoing Equifax breach, representatives from these specific firms were urged to testify before Congress. These firms were adversely affected by the attack on Equifax, most likely due to the immediate consumer response of freezing credit across all three agencies and to common concerns about the regulatory response. In addition to investigations currently being undertaken by the Federal Trade Commission, the Senate Finance Committee, and other organizations, the Consumer Financial Protection Bureau announced in September 2017 that it will implement "a new regulatory regime" for credit-rating agencies, requiring that each firm host regulators, who would be embedded at the firm, in order to prevent future breaches. Moreover, the data breach probably caused investors to lose confidence in the agencies' cyber protection to revise up the probabilities of future data breaches. An equal-weighted portfolio of TransUnion and Experian experienced negative CAR of over 18 percent in the seven trading days following the announcement, with a t statistic of –4.7 (figure 7-5).

We also observed the breach's negative impact on corporate customers. As consumers freeze credit, the data breach would have a negative impact on firms that use the credit rating agencies' ratings to provide consumer credit. The economically linked firms that we identified through news searches include Fair Isaac Corporation, Synchrony Financial, Fidelity, and Virtu. An equal-weighted portfolio of these firms experienced a negative CAR of more than 9 percent in the seven-day window (figure 7-6).

Attacks through the Weakest Link in the Supply Chain

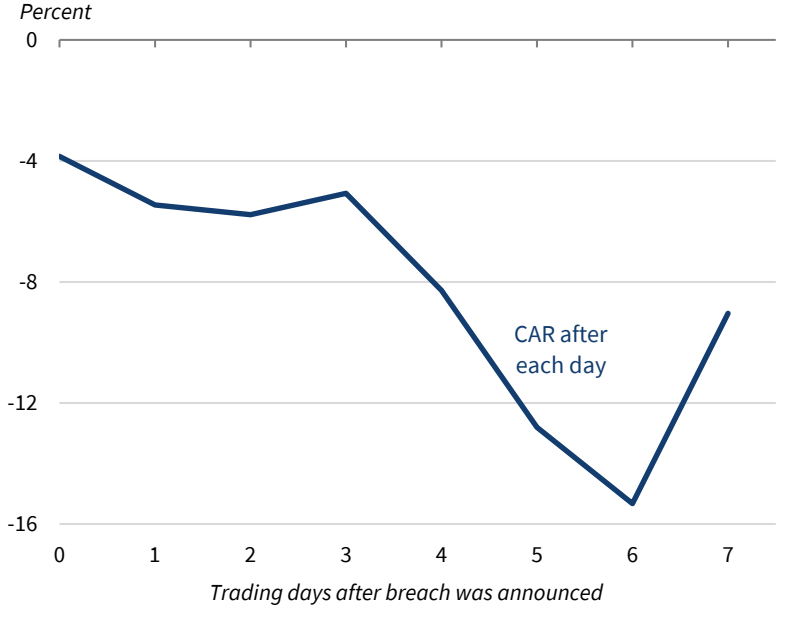
A firm's security flaw can put its customers, suppliers, and corporate partners at risk. PwC (2014) states that "sophisticated adversaries often target small and

Figure 7-5. TransUnion's and Experian's Cumulative Abnormal Returns After Equifax's Data Breach Announcement



Sources: Bloomberg; CEA calculations.

Figure 7-6. Portfolio of Finance Firms' Cumulative Abnormal Returns After Equifax's Data Breach Announcement



Sources: Bloomberg; CEA calculations.

Box 7-5. Supply Chain Attack: Home Depot

The Home Depot data breach occurred from April to September 2014, and it compromised the information of roughly 56 million unique payment cards and 53 million email addresses (Home Depot 2014a, 2014b). The hackers entered Home Depot's payment systems through the use of a third-party vendor's login information and then unleashed malware to gain access to the company's point-of-sale devices (Home Depot 2014b).

The data breach had a long-term negative impact on Home Depot, and also on other firms that were exposed to the hacked point-of-sale devices. Since 2014, Home Depot has incurred losses of roughly $300 million due to the data breach (Home Depot 2017). Net of insurance payments, the company has spent $200 million to provide credit monitoring for affected customers, and it also had to hire additional staff for its call center, investigate and upgrade its security network, and pay fines and legal fees related to the breach (Home Depot 2017). The breach also affected card issuers, whose customers had to be reimbursed for fraud and whose cards had to be reissued. The Credit Union National Association (CUNA 2014) estimates the cost of these remedies at $8 per affected credit card, thereby placing the direct cost incurred by the industry as the result of the data breach at $440 million.

medium-sized companies as means to gain foothold on the interconnected business ecosystems of larger organizations with which they partner." This type of breach, which is known as a supply chain attack, is one of three main vectors whereby hackers penetrate system defenses, accounting for over 60 percent of all adverse cyber events suffered by companies in 2016 (*Wired* 2015; Accenture 2016). By exploiting a weakness in a relatively small and weakly protected supplier, hackers can bypass even robust cybersecurity measures. An advantage of this attack vector is that cybercriminals can blend in with regular network traffic, including by using legitimate credentials harvested from the vendor. A large-scale data breach suffered by Home Depot is an example of a supply chain attack (box 7-5).

Realizing the importance of the safety of the entire supply chain, the industry is finding solutions to ensure supply chain safety. McAfee (2017) notes that multiple authentication methods—such as a second factor authentication using a hardware token or mobile app, including for vendor access—may help prevent cyber breaches across the supply chain. After facing a cyber breach originating from a supplier, Target announced several supply chain security measures in line with NIST standards, such as limiting vendors' access to the network and improving authentication methods, in addition to broader cybersecurity measures, such as improving the monitoring of the cyber network (Target 2014). As part of the conditions for its 2017 settlement with the affected credit unions, Home Depot committed to industry standard risk

Box 7-6. Exploiting Cyber Vulnerabilities to Attack a Third Party: Mirai Botnet

A high-profile example of hackers exploiting cyber vulnerabilities came in 2016, when cybercriminals began using the Mirai source code to launch broad-ranging DDoS attacks on various targets. According to an analysis published by the Institute for Critical Infrastructure Technology, Mirai exploited devices that work with the Internet of Things with factory default or hardcoded user names and passwords and used them to create and build a botnet (an army of computer devices), which then overwhelmed numerous targets with traffic (Scott and Spaniel 2016). In October 2016, the Mirai Botnet was deployed against the Internet infrastructure company Dyn, which provides critical technology services for websites including Twitter, Amazon, Tumblr, Reddit, Spotify, and Netflix (Krebs on Security 2016). For much of the day, access to each of these websites was curtailed, as Dyn's servers were repeatedly overwhelmed by malicious traffic launched from hacked devices that work with the Internet of Things (Krebs on Security 2016). In a statement made after the attack, Dyn described the Mirai botnets as the primary source of malicious attack traffic that halted Internet use (Dyn 2016).

exception processes, as well as periodic security compliance assessments of those vendors with access to card payment information. This reflects broader trends within the market, such as the establishment of platforms like CyberGRX (www.cybergrx.com), which serve as clearinghouses of information on the risks posed to downstream firms by the underlying cybersecurity weakness of their upstream partners (Patterson Belknap 2017). In addition, the American Bar Association has created a Vendor Contracting: Cybersecurity Checklist to inform information security concerns in the procurement process (ABA 2016). As another example of reducing cyber risk in the supply chain process, a consortium of financial services companies—including Bank of America, JPMorgan Chase, Wells Fargo, and American Express—established a company, TruSight, to standardize the risk assessment of third-party suppliers and partners, including of their information security (Trusight 2017).

Using Cyber Vulnerabilities to Usurp Resources and Launch Attacks on Other Firms

A cyber threat actor may exploit inadequately protected devices to launch external attacks against a third party. Devices that work with the Internet of Things are notoriously unsecure, because their manufacturers aim to speed up adoption by cutting costs, and the most commonly cut cost is that of security protection. The Mirai Botnet attack, described in box 7-6, is an example of a cybercriminal using an existing security vulnerability to launch an attack against a third party.

Economy-wide Spillover Effects from Firms with Critical Infrastructure Assets

Finally, and perhaps most important, if a firm owns a so-called critical infrastructure asset, an attack against this firm could cause major disruption throughout the economy. The 2013 Presidential Policy Directive-21 (PPD-21), "Critical Infrastructure Security and Resilience," notes that 16 critical infrastructure sectors that are critically important to both the U.S. economy and national security. These sectors include chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emerging services, energy, financial services, food and agriculture, government facilities, healthcare and public health, IT, nuclear reactors, materials, and waste, transportation systems, and water and wastewater systems (DHS 2017b). On January 6, 2017, DHS designated the U.S. election systems as a subsector of the existing government facilities critical infrastructure sector (U.S. Election Assistance Commission 2017). Insufficient cybersecurity investment in these sectors exacerbates the risks of cyberattacks and data breaches. The economic implications of attacks against critical infrastructure assets are described in more detail later in the chapter.

The presence of externalities would lead firms to rationally underinvest in cybersecurity. Left to their own devices, firms will choose their optimal level of investment by conducting an analysis of private costs and benefits without taking externalities into account. In light of this market failure, regulators are likely to devise a scheme of penalties and incentives that are designed to make firms internalize the externalities and thereby help raise levels of cybersecurity investment to the socially optimal level. For example, certain mandatory disclosure requirements were previously shown to incentivize firms to adopt better business practices (see, e.g., Gordon et al. 2015, who conduct an analysis of externalities resulting from weak cybersecurity).

Common Vulnerabilities

In this section, we explore how shared usage of technologies creates common vulnerabilities across firms. These common vulnerabilities create a high likelihood that multiple firms may be compromised by a bad actor taking advantage of the same vulnerability in several firms. Common vulnerabilities create high correlations in firms experiencing adverse cyber events. This matters for two reasons. First, when news of one firm experiencing a cyberattack or a data breach become public, very likely other firms have experienced the same compromise, even though they may not have revealed it publicly. Second, the high correlation in adverse cyber events creates difficulties for insurers in constructing diversified portfolios of insured firms; we will discuss this point later in the chapter.

Corporate computer systems and networks are vulnerable to compromise at multiple layers, including software, firmware, and hardware. When a vulnerability in one of these layers is discovered and subsequently exploited by cybercriminals or other malicious actors, it is highly probable that other firms that use the same technology may be similarly vulnerable. Malicious actors often target a vulnerability wherever it exists, not necessarily focusing on a single firm or industry. In what follows, we explain how common technologies can create common vulnerabilities across multiple firms.

Software

A computer's software is any data or computer instructions stored on a computer's hardware. Software is encoded in a binary basis and forms the tools by which computers execute tasks and manipulate information. In vulnerable systems, unbeknownst to the end user, software can be modified or otherwise abused by malicious actors to run unwanted processes on a given system, allowing the actors to affect adverse outcomes for a system's users. If undetected, these processes may allow an adversary to obtain or manipulate information on a computer system without the end user's permission. The goal of these adverse actors is often to enable unauthorized access to secure systems for the purpose of stealing, encrypting or destroying private data and information, or for modifying industrial control processes in order to cause harm to a company's physical assets and/or its employees.

Software vulnerabilities often stem from simple errors in software coding. Unbeknownst to developers, innocent coding errors may make a program vulnerable to software exploits. In a typical software code, there are an average 25 errors per 1,000 lines of code (NIST 2016). NIST has stated a goal for a "dramatic reduction" in software vulnerabilities. The stated goal is to reduce the error rate to 25 errors per 100,000 lines of code (NIST 2016). Systems with near-zero errors are produced routinely today in the aerospace industry, but at several times the cost of ordinary software. This objective will have substantial costs associated with its implementation, but ultimately will hopefully pay off through a sufficient reduction in software vulnerabilities.

We now discuss the particularly harmful so-called zero-day vulnerabilities, for which a security solution does not yet exist, and the "backdoor" methods that malicious actors exploit to gain entry into a seemingly secure system.

Zero-day vulnerabilities. So-called zero-day vulnerabilities are a particular subset of vulnerabilities characterized by being unknown to the hardware/software vendor and end users prior to being discovered and/or exploited. "Zero" days refer to the amount of time in which a producer or cybersecurity firm has from the time of discovery to provide the users with a patch to eliminate the vulnerability.

Zero-day vulnerabilities are often exploited with the help of the so-called exploit kits, primarily available for purchase on the so-called dark web—which

refers to the large portion of the Internet whose contents are not indexed by standard search engines. An exploit kit is a web-based application centered on a zero-day vulnerability that streamlines the vulnerability's exploitive application; these kits provide easy to use, replicable templates to exploit individual vulnerabilities on a large scale. A typical kit contains mechanisms to profile potential victims, identify compromised systems, and subsequently deliver "payloads" (exploitative or malicious software).

Once a patch is written and released by the architects, the vulnerability is no longer deemed a zero day. However, it is ultimately up to the end users to update their systems in order to be considered immune to a given zero day vulnerability. Lloyd's of London (2017) notes that it can "take anywhere from days to years" before a developer is made aware of the vulnerability. This allows illicit discoverers of vulnerabilities ample time to explore angles of compromise, develop the necessary software for exploitation, and potentially market this exploitation technique to interested third parties.

"Backdoor" access. A backdoor is defined as a "hidden entrance to a computer system that can be used to bypass security policies"; it may allow one to gain access to a network a computer system or a connected device, unbeknownst to the end user (OWASP 2006). It is common for a commercial software package to have a backdoor to enable developers to modify the systems they oversee. A backdoor may take the form of a hidden aspect of a program, a separate program, a part of an operating system, or even be coded into the firmware already installed on a system's hardware. Threat actors may gain access to pre-installed backdoors or install their own backdoors with the end goal of taking control of the systems or inserting malicious modification at any time that they wish. Many hardware products have backdoor methods of access and may be vulnerable to security compromises using these backdoors methods of entry, regardless of the software programs that are being run on the hardware in question.

Firmware

Firmware constitutes the next step above hardware in a traditional system stack. System firmware is usually software that boots or initiates systems, along with running baseline-level tasks, such as power management and end-user controls (e.g., mice or keyboards). This software is often unique to or integrated with individual firms' hardware, thus earning the moniker "firmware" due to being hardware specific to a given firm's technology. USB drives, hard and solid-state drives, memory cards, and digital power chargers all typically utilize firmware.

Firmware is a prime target for compromise because it resides below the operating system and may not be protected by the security software that runs on an operating system. These firmware vulnerabilities, which allow attackers to take control of a system during its booting phase, have been identified in

USB devices (e.g., memory sticks), network cards, embedded and keyboard controllers, baseboard management controllers, modems, central processing units batteries, home routers, office printers, IP phones, and many other devices. McAfee has identified several instances of hacking groups, industrial espionage teams and organized crime groups, utilizing firmware exploits in order to commit cyberattacks and cyber theft.

Hardware

A computer's hardware are the physical components of a computer. Hardware components can be either active (internally powered) or passive (driven by an external power source). Typical components include, but are not limited to, monitors, keyboards, hard and soft drives, graphics cards, sound cards, processors, and motherboards. Although traditionally harder to attack externally, hardware vulnerabilities can completely undermine an entire system stack's security. Hardware threats undermine a system's software security measures because software inherently assumes that hardware on which it runs is not compromised. The discovery of a hardware-based exploitation may force system infrastructure to be replaced entirely as hardware compromises typically cannot be fixed by software patching alone.

Hardware is a less frequent target of hackers than software for a number of reasons: hardware is typically less easily accessible, it is not as well understood, and attacks against hardware often must be highly specialized. However, once discovered, hardware vulnerabilities can be highly damaging: Hardware vulnerabilities may cause compromises independent of operating system or software security measures.

A striking recent example of a hardware vulnerability was recently discovered by the Project Zero (2018) research team at Google in certain processors manufactured by Intel, AMD, and ARM. Specifically, Google found and reported three unique vulnerabilities usable against these processors to the processors' respective manufacturers on June 1, 2017.[6] The vulnerabilities could allow malicious actors to steal information stored in a processor's memory, affecting virtually all computing devices, such as personal computers, cloud servers, and smartphones.

Cloud Computing

Cloud computing has allowed companies to achieve economies of scale by outsourcing various tasks—such as data storage, services, and analytics—to outside providers. McAfee (2017) cites that 93 percent of organizations utilized some form of cloud computing for software, platform, or infrastructure services.

[6] These vulnerabilities are registered as CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754 with the National Vulnerability Database's Common Vulnerabilities and Exploits list.

Cloud computing platforms use the virtual machine archetype; a virtual machine simulates a physical computer system (hardware, operating system, and applications) on top of an underlying operating system. A cloud can be running any number of virtual machines simultaneously on top of its underlying operating system, allowing for providers to utilize the same hardware for different customers without usage conflicts between end users. The programs overseeing this delegation of space for different virtual machines are called "virtual machine monitors" or hypervisors.

Cloud computing has its own inherent vulnerabilities, which can create common risks among end users. If the underlying hypervisor overseeing a cloud network is compromised, it can be assumed that all systems being hosted on the network will in turn be vulnerable to exploitation. This leads to a great degree of risk correlation between firms from cyber threats that otherwise would not exist if the firms' data and services were located locally. Furthermore, if a hardware replacement or hard-software update (a software update that requires a power reset) is needed to resolve these problems, computing jobs need to be interrupted, which upsets customers and in turn discourages hosts from running these time-consuming updates or patches.

Managed service providers (MSPs) are similar to cloud computing providers, but they typically provide additional IT services, such as network connectivity, data security solutions, and general IT strategy management. According to a 2017 report by PwC, multiple MSPs were targeted from 2016 onward by a single adverse actor, APT10 (PwC 2017). (According to FireEye, a cybersecurity firm, APT10, is a Chinese cyber espionage group that FireEye has tracked since 2009.) PwC (2017) further states that as a result of its activities, APT10 has potentially gained access to "the intellectual property and sensitive data of those MSPs and their clients globally" (PwC 2017).

The Problem of Insufficient Data

In today's data-driven world, important investment decisions are based on sound empirical analysis. However, the field of cybersecurity is plagued by insufficient data, largely because firms face a strong disincentive to report negative news. Cyber protection could be greatly improved if data on past data breaches and cyberattacks were more readily shared across firms.

There are multiple reasons for insufficient disclosure. To being with, many cybersecurity breaches go undetected by firms. Citing data from cybersecurity firms, PwC (2014) reports that as many as 71 percent of cyber compromises go undetected. Furthermore, according to industry reports, the U.S. government can frequently observe an attack. For example, the Center for Strategic and International Studies (2014) reports that in 2013 U.S. government notified 3,000 companies that they had been hacked. Even when a firm is aware that it had experienced an adverse cyber event, it would frequently refrain

from reporting the event for fear of negatively affecting its market value and its relationships with corporate partners. For example, the Center for Strategic and International Studies (2014) reports that when Google was hacked in 2010, another 34 *Fortune* 500 companies were hacked at the same time (that fact eventually became public knowledge through WikiLeaks), but only one of these companies reported publicly that it had been hacked.

Data on adverse cyber events that involve breaches of PII and a subset of other security breaches are slowly becoming available, partly due to disclosure requirements. Countries around the world are adopting mandatory data breach disclosures, for compromised PII on firms' customers (though at different levels of coverage), such as the General Data Protection Regulation (GDPR) in the European Union. The U.S. government also imposes sector-specific cyber disclosure legislation. The Health Insurance Portability and Accountability Act (HIPAA), pursuant to Public Law 104-191, sets disclosure requirements on personal data protection, though studies have raised concerns about compliance with, exemptions to, and the lack of, "standardized technology requirements" in the regulations (Chang 2014; Koch 2017). Banks and certain financial institutions are subject to regulatory examinations that include review of their safeguards for protecting the security, confidentiality, and integrity of consumer information, which include disclosure requirements in the event of a breach. The Department of Energy also requires disclosure of events—including those that are cyber-related—that may have an impact on the electricity system, through the OE-417 Electric Emergency Incident and Disturbance Reports, pursuant to Public Law 93-275. These reported incidents are posted on the Department of Energy's website, which gives information on the event's date, date of restoration, areas affected, alert criteria, event type, demand loss, and number of customers affected. Of 141 events reported in 2016, 5 were cyber-related. Of the 127 events reported in 2017, two were cyber-related, though these events were not reported to affect customers or result in the loss of demand (DOE 2017).

For publicly traded firms, public disclosure of materially important adverse cyber events is mandated by the Securities and Exchange Commission's (SEC) 2011 Guidance, and also by the requirements that trigger the filing of the SEC's Form 8-K. Specifically, the 2011 Guidance mandates that publicly traded firms disclose "material" cybersecurity risks and cyber incidents. However, the effectiveness of the SEC's 2011 Guidance is frequently questioned. There are concerns that companies underreport events due to alternative interpretations of the definition of "materiality" (Gordon et al. 2006, 2015). There are also concerns that the disclosure requirements are too general and do not provide clear instructions on how much information to disclose, and that they therefore "fail to resolve the information asymmetry at which the disclosure laws are aimed" (Ferraro 2014). For example, according to the 2017 survey of 2,168 individuals who were involved in both cyber risk and enterprise risk management

activities in their firms, 36 percent of survey participants said that a material loss of information assets does not require a disclosure on the firm's financial statements. At the same time, 43 percent of respondents stated that their firm would disclose a loss of property plant and equipment on its financial statements (Ponemon 2017b). According to these studies, more comprehensive and mandatory disclosure guidance, such as through legislative endorsement (Ferraro 2014) or endorsement by the SEC (Gregory 2014), may help overcome these issues.

If, between quarterly reports, a cyberattack or a data breach triggers an event that would mandate the filing of Form 8-K (e.g., bankruptcy, departures of corporate directors, entry into or a termination of a "material definitive agreement"), then victims must disclose the cyber event under the requirement that the firm file the form within four business days of the event. If a materially important cyber event is privately disclosed by the affected firm to a financial intermediary—such as a buy- or sell-side analyst, an investment manager, a broker dealer, or an investment adviser who could generate a profit for themselves or their clients from having this informational advantage—Regulation Fair Disclosure requires that the event must be disclosed to the public promptly.

Other countries also mandate disclosures of cyber breaches, and some countries have stricter disclosure requirements than the United States does. For example, in April 2016 the European Union adopted GDPR, which becomes effective in May 2018 and mandates companies to disclose data breaches. This regulation expands the scope of the EU's 1995 data protection regulation to all companies that process the data of EU-based subjects, regardless of the company's location. Past regulations only applied to companies based on their physical location, and the new regulation will also affect United States–based firms as long as they have European customers. Companies subject to this regulation must notify their customers and other affected parties of breaches where "a data breach likely to result in a risk for the rights and freedoms of individuals" (GDPR 2017). The breach must be disclosed to the government, customers, and controllers within 72 hours of the firm's becoming aware of the breach. This new rule will further increase the number of publicly reported data breaches.

Even if cyber events are not being disclosed by firms, the news media can find out about such events through journalist investigations. For example, Verizon (2017) reports that 27 percent of data breaches were discovered by third parties. These third parties may notify the news media in addition to notifying the affected firms, creating another channel for the spread of information.

The lack of a representative data set for cybersecurity incidents poses a number of challenges to firms and policymakers. For policymakers, it makes it next to impossible to accurately measure the cost of cybersecurity incidents for the U.S. economy and to determine whether more active government

involvement is needed to limit cybersecurity risk. Likewise, for firms, the lack of data makes it difficult to correctly assess the expected costs of cybersecurity exposure and to determine the optimal level of investment in cybersecurity. Moreover, when negative information is underreported for incentive reasons, agents may erroneously assume that the negative information/events simply do not exist (see, e.g., Scherbina 2008). In case of adverse cyber events, underreporting may lead the less sophisticated managers to assume that the risk is not significant and consequently to underinvest in cybersecurity. Industry sources speculate that less sophisticated smaller firms underinvest in cybersecurity for this reason.

Unlike firms and private individuals, cyber insurance and cybersecurity providers have the advantage of being able to collect data on cyberattacks and data breaches through their business operations. However, these entities are reluctant to share their data with the public because of privacy concerns for their clients and also because these data represent a source of competitive advantage in providing security services for cybersecurity companies and in pricing cyber insurance products for insurance companies.

A more robust data set on cyber incidents and cyber threats that could be updated in real time would greatly help firms improve their cybersecurity. And still another negative effect of the paucity of publicly available data is that it may slow the development of a more competitive market for cyber insurance.

Dark Cyber Debt

As discussed above, firms are reluctant to reveal cyber breaches to the public for fear of lowering their valuations; even when a firm's management does report a breach, it often underreports its scope. Most likely, the information about the breach will eventually become public, at which point the value of the firm will decline to reflect the resulting monetary losses. In this section, we introduce the concept of "dark cyber debt" to describe the future negative valuation impact of a breach that a firm hid from the public. It is "dark" because it is currently hidden, and it is a "debt" that eventually would need to be paid before investors are paid.

Consider the latest illustration of the concept. In October 2016, the personal data of approximately 57 million customers and drivers was stolen from Uber Technologies Inc. (Newcomer 2017). The data were then ransomed back to Uber in exchange for an illicit payment of $100,000 to the hackers by Uber's security chief and one of his deputies (Newcomer 2017). The compromised data included some 600,000 driver's license numbers for Uber's drivers, which were linked to their identities (Newcomer 2017). Though Uber has admitted it had a legal obligation to disclose the attacks on a timely basis to regulators and also to the drivers whose identities were compromised, it instead chose to hide the news and to pay the perpetrators to delete the stolen sensitive information

(Newcomer 2017). Further attempts to conceal the damage manifested themselves through Uber's executives writing off the $100,000 as a "bug bounty," a practice whereby technology companies hire external parties to attack their software in order to test for vulnerabilities (Isaac, Benner, and Frenkel 2017). It is now clear that these breaches were the work of criminals rather than firms hired to test Uber's cybersecurity. The timing of Uber's hack was particularly unfortunate, because the firm had been planning to go public. In the aftermath of the news, SoftBank, a Japanese firm, and a group of Uber's shareholders agreed to a deal valuing the company at $48 billion, a notable decline in the $70 billion that Uber commanded just over a year ago (Reuters 2017b). Although not all the decline in value can be attributed to the data breach, given that Uber also faced other types of negative publicity, offers following the hack were substantially lower than pre-breach figures.

This particular nondisclosure is far from the only example of dark cyber debt. For example, in 2016 Uber faced a $20,000 fine for its failure to disclose a 2014 breach (New York State Office of the Attorney General 2016).[7]

Cyber Insurance

The rise in malicious cyber activity directed at firms over the past decade gave an impetus to a quickly growing market for cyber insurance. The global cyber insurance market is estimated to be worth roughly $3.5 billion today, up from less than $1 billion in 2012, and is projected to grow to $14 billion by 2022 (Lloyd's of London 2017; Allied Market Research 2016).[8] North America, particularly the United States, accounts for roughly 90 percent of the global cyber insurance market. In 2016, property and casualty insurers wrote $1.4 billion in direct premiums for cyber insurance, up 35 percent from the previous year (Lloyd's of London 2017). This figure, however, is only a miniscule fraction of the roughly $530 billion in premiums for the entire insurance market. Although the U.S. market is more developed than markets in other countries, only about a third of U.S. companies have purchased some sort of cyber insurance, with large variation across sectors (Romanosky et al. 2017). Though supply and demand for cyber insurance continues to grow, the cyber insurance market faces a number of challenges that slow down its pace of development.

Compared with other risks covered by insurance—such as wind, flood, and fire—cyber risk is perhaps the fastest-evolving and least understood. A big challenge faced by the market is the scarcity of data on past incidents. The importance of modeling cannot be understated when it relates to pricing risk,

[7] Attorney General of the State of New York, Internet Bureau, Assurance No. 15-185. We must note that even when a company takes all reasonable cybersecurity measures and makes appropriate disclosures, its stock price will likely decline when a data breach becomes public.

[8] Our discussion of cyber insurance and cyber insurance policies only includes specialized cyber insurance policies marketed as such. It does not include other broader policies that may cover losses from a cyber event.

and the lack of historical data and unpredictability of risk make it difficult to model and therefore underwrite. There is a significant qualitative aspect to pricing that insurers rely on when pricing policies. As a result, policies for cyber risk are more customized than other risk insurers taken on, and, therefore, more costly (NAIC 2017). Insurance firms also need to be able to assess the correlation in risks and losses across firms in order to form diversified portfolios of insured firms. Cyber insurance, like most insurance products, distinguishes between two loss categories, first party and third party. First-party losses are those that directly harm the insured, while third-party liability relates to claims undertaken by external parties who experience losses due to the insured's actions. Without good data, it is very difficult to quantify the potential spillover effects to third parties. Firms that got into the cyber insurance market early clearly have a data advantage over new entrants by having collected historical data of past cyber insurance claims from client firms. However, the "data barrier" makes the market less competitive by deterring new entrants.

Some insurers utilize information from policyholders' self-assessment forms to place a firm's risk into a generic high, medium, or low level. The varying levels of information that insurers possess on each of their clients determines the size and sophistication of their respective policies and explains the differences in coverage among firms. Some insurers have admitted to relying on other insurance companies' premiums to determine pricing, due to a lack of their own data. The adverse effect of insufficient data is that insurance firms struggle to price cyber risk. Underpricing cyber risk could result in insurers being unable to cover claims. Overpricing cyber risk could lead to underinsurance on the part of the firms.

A systematic collection of data on past cyberattacks and data breaches would be a big push for a quicker development of the cyber insurance market. Currently, companies are required to publicly report data breaches that expose personally identifiable information, payment data, or personal health information. However, there are no mandatory reporting requirements for other types of cyber events, such as those involving IP theft, ransoms, data and equipment destruction, or business disruption. Though publicly traded firms are required to report cyber events that have the potential to materially affect the firm's value, there is substantial underreporting, as firms are free to determine themselves whether an event is "materially important" (Jin 2015). The absence of data on cyber risk and the difficulty of monitoring firms' behavior have resulted in insurability challenges for the cyber insurance market. Because of this, general challenges to all insurance markets (adverse selection and moral hazard) exist as companies that have been victim to a serious malicious cyber activity are more likely to buy insurance, and having insurance fosters a lack of incentive to invest in self-protection measures.

Another major reason the cyber insurance market is relatively small in size is due to the relatively high premiums for relatively limited coverage.

Box 7-7. Target's Cyber Insurance Policy

In 2013, Target experienced a data breach in which payment information and customer data were stolen. Between 2013 and 2015, Target's cumulative losses for this incident were $290 million (Target 2017). These expenses included legal and other professional services related to the data breach, but did not include insurance compensation for the potential reputational damage. Insurance coverage offset only $90 million of the losses, resulting in a net pretax loss of $200 million (Target 2017). Thus, Target's cyber insurance only provided coverage for about 30 percent of the easily quantifiable data breach costs. Of course, because the out-of-pocket costs were used to lower Target's tax liability, the after-tax losses were somewhat lower (SEC 2017).

Typically, only costs that can be easily quantified are covered by insurance. The most frequent type of cyber insurance coverage today relate to data breaches, including first-party coverage for costs such as crisis management and identity theft response and third-party coverage related to privacy liability. Other common types of first-party loss coverage include costs related to investigations of the attack, restoring business services, credit-monitoring services, notifying affected parties, ransom payments, and other losses associated with business disruption. It is uncommon for cyber insurance to cover reputational harm, loss of future revenue, costs of improving cybersecurity systems, losses from IP theft, and nation-state attacks.

The ambiguity of coverage for cyber insurance products, which is also limited, coupled with the heterogeneity of offerings across insurance firms, is another challenge faced by the burgeoning cyber insurance market. The lack of standardization of insurance products makes it difficult for firms to compare coverage across insurance firms. This, in turn, is another reason for the slow adoption of cyber insurance coverage.

As a result of underreporting of cybersecurity incidents and the associated costs, firms may underestimate their own risks, and the demand for insurance may be lower than optimal. Moreover, insurance firms themselves may be unwilling to provide sufficient limits for cyber insurance. The case study given in box 7-7 describes how only a small portfolio of losses stemming from Target's 2013 data breach was covered by insurance (Naked Security 2015).

Luckily, the passage of time will allow insurance companies to collect sufficient data from their clients to better price insurance products and to expand coverage. A competitive cyber insurance market that offers a wide array of efficiently priced products would become an important contributor to economic growth. Though publicly traded firms enjoy a diversified set of investors, who do not demand to be compensated for the idiosyncratic risk associated with cybersecurity breaches and attacks, the cyber insurance

market should allow private firms to cross-insure their cyber risk and lower their cost of capital. Cyber insurance will help reduce the deadweight losses that are associated with corporate bankruptcies driven by cyberattacks and data breaches. Another advantage of the cyber insurance market is that through the underwriting process, it may encourage the adoption of better cybersecurity practices. The insurance provider's ability to assess whether a potential policyholder has adequate cybersecurity incentivizes the firm to undertake cybersecurity investment. Premiums would generally be higher for firms that do not have any substantial cybersecurity measures. This mitigates moral hazard in the marketplace.

However, the cyber insurance market will continue to face challenges. Cyber threats are ever evolving. Increasing reliance on information, increasing interconnectedness, and the adoption of new technologies will bring about new cyber threats. Thus, even after collecting sufficient data on past cybersecurity events, predicting risks and correlations will remain a challenge.

By offering protection against theft, cyber insurance will reinforce firms' incentive to invest in IP and proprietary data. However, it will be difficult to achieve complete protection, for two reasons. First, as discussed above, firms may often be unaware that they have been breached. Second, coverage of third-party losses will continue to be limited, due to firms' reluctance to admit that they have been breached.

The Costs of Malicious Cyber Activity for the U.S. Economy

The losses suffered by the corporate sector as a result of cybersecurity breaches and attacks extend beyond the direct losses suffered by firms that are targeted. These additional costs arise from (1) spillover effects to economically linked firms, (2) the ever-increasing expenses for cybersecurity, and (3) the drag on economic growth caused by cyber threats. We describe these costs in more detail in this section.

A cyberattack or data breach experienced by a firm is likely to have significant spillover effects on its corporate partners, employees, customers, and firms with a similar business model. As we highlighted in the case of the Equifax attack, stock prices of firms that have a similar business model and of firms that rely on Equifax data also declined in response to the news of the data breach.

Firms also incur nonnegligible costs associated with preventing cyber incidents, and they must acquire security products (spam filters, antivirus protection), offer services for consumers (training), and engage in other fraud detection / tracking efforts (Anderson et al. 2012). The investment bank Morgan Stanley (2016) estimates that the global IT security product and services market will grow by 18 percent each year between 2015 and 2020, to become a

$128 billion market by 2020. We estimate that the Equifax data breach resulted in significant share price increases for cybersecurity firms. This implies that market participants revised up their expectations of the cybersecurity firms' future revenues. We are reluctant to ascribe the cost of cybersecurity protection to a deadweight cost to the U.S. economy. Employment and output in the cybersecurity sector contribute to economic growth. Innovative technology solutions developed by the sector may generate positive spillover effects elsewhere in the economy. A sophisticated cybersecurity sector could become a reliable source of exports for products and services many years to come.

Finally, malicious cyber activity imposes a drag on economic growth by enabling theft of IP and by slowing the speed of the adoption of new technologies. Lacking sufficient protection, firms will underinvest in research and development, slowing the pace of innovation. Additionally, ever-evolving cyber threats slow down the rate of development and adoption of new types of information and communications technology, and thereby lower the efficiency gains that can be achieved with these new technologies (for a detailed discussion and analysis of this and related issues, see Hughes et al. 2017).

When estimating the total economic costs of cybersecurity incidents against the U.S. economy, one should not overlook the substantial direct cost imposed on the government sector. Using a data set of cyber incidents from Advisen, a for-profit organization that collects and resells data from the commercial insurance industry and public news sources, Romanosky (2016) estimates that government agencies are at a highest risk for a cyber incident (risk is defined as the number of cyber incidents divided by the number of firms/agencies in a sector).

According to the Government Accountability Office (GAO 2017), Federal agencies reported a 58.9 percent increase in the number of cyber incidents between fiscal years 2012 and 2015 (the most recent year available). In a highly publicized incident, between 2014 and 2015, the Office of Personnel Management (OPM 2015) suffered a system breach, in which security data from submissions of Form SF-86 were breached for 21.5 million individuals, including 5.6 million sets of fingerprints. Another separate cyber incident involving personnel records occurred in 2015, which affected 4.2 million individuals (OPM 2017).

The government incurs substantial, though not easily quantifiable, costs of IP theft and theft of information pertaining to national security. The case study of the IP theft for the F-35 fighter plane described in box 7-8 illustrates a very costly cyber theft from the U.S. government (Capaccio 2017).

Evidence from State and local governments suggests that cyber risks are also pervasive at these levels. Data breaches or compromises have the potential to affect thousands or even millions of individuals through the release of personal or sensitive information or disruptions of government service provision. Responses to a 2013 survey of State and local government officials

Box 7-8. The Theft of U.S. Military Secrets through Cyber Means: the F-35

The F-35 is a single-seat, single-engine fighter aircraft that was developed primarily by Lockheed Martin to be used by the U.S. armed forces, as well as allied countries. The plane is optimized for use as a multirole fighter, with the ability to perform air-to-air; air-to-ground; and intelligence, surveillance, and reconnaissance missions. Program development officially launched in 2001, and deliveries began in 2011. The program's cost to complete is estimated at more than $400 billion (*Wall Street Journal* 2014).

It has since been verified that these malicious cyber activities were carried out by foreign agents, with the Chinese national Su Bin pleading guilty in 2016 to stealing data related to the F-35 and seeking financial gain by selling the illegally acquired data (DOJ 2016c). As noted by Department of Defense Undersecretary Frank Kendall, these breaches could "give away a substantial advantage" and "reduce the costs and lead time of our adversaries to doing their own designs" (DOJ 2016c). This appears to have been the case, because observers have noted that the J-31, a Chinese stealth fighter introduced in 2014, appears to have been modeled on the F-35 (Weisgerber 2015). If the Chinese did use designs stolen from U.S. contractors, it could have allowed them to cut down significantly on the $350 billion spent by the United States through fiscal year 2017 on the F-35's development and production (DOD 2015c).

suggested that officials often underestimate the prevalence and potential severity of adverse cyber events (Center for Digital Government 2014), and Security Scorecard's 2016 Cybersecurity Report ranks government (Federal, State, and local) at the bottom of 18 major industries in terms of cybersecurity (Security Scorecard 2016). Data on the number of data breaches at government entities do not show rates of increase that give particular cause for concern, but trends in the affected numbers of individuals could potentially be quite different. According to a recent survey of IT and security management professionals in State and local government, 40 percent of respondents indicated that the number of cyber incidents associated with malware had increased over the preceding year (Center for Digital Government 2014).

Cyber threats impose significant costs on private individuals. Cyber intrusions that steal PII from the corporate and government sectors generate welfare losses for those uninsured individuals whose private information is stolen. Attacks against State and local governments, furthermore, have a negative impact on households that rely on the services provided by the government entities. Finally, individuals are frequent direct targets of cybercrimes committed via email and the Internet. The FBI's Internet Crime Complaint Center provides the public with a mechanism to report Internet-facilitated criminal

activity. In 2016, this center received nearly 300,000 individual complaints of cybercrimes, with an estimated total cost in excess of $1.3 billion. Among the most costly crimes targeted at individuals were confidence and romance frauds. These attacks cost victims $220 million in 2016, and were carried out by criminals posing as a close family member or romantic partner for the purpose of convincing victims to send money or personal information. Moreover, the agency also estimates that only 15 percent of cyber-related criminal activity is reported each year, so actual damages are likely significantly higher.

It is difficult to estimate how much malicious cyber activity costs the U.S. economy because, as discussed above, many events go undetected—and even when they are detected, they are mostly unreported or the final cost is unknown. After accounting for the negative spillover effects, the CEA (2018) estimates that breaches and attacks cost the U.S. economy between $57 billion and $109 billion in 2016, which amounted to almost 0.31 percent to 0.58 percent of that year's GDP. The Center for Strategic and International Studies (2014) computes the global cost of malicious cyber activity as between $375 billion and $575 billion. The report further estimates that the cost of malicious cyber activities directed at U.S. entities was $113 billion in 2013, which represented 0.64 percent of GDP that year. Aggregating information from a variety of industry studies, MIT (2015) comes up with an estimate of a similar magnitude for the global cost of adverse cyber events, about $400 billion a year.

Devastating Cyberattack Scenarios

Cybersecurity professionals, in both the private and public sectors, stress that the potential costs of malicious cyber activity could far exceed the ongoing costs suffered by the U.S. economy. After the worst terrorist attack in U.S. history, the 9/11 Commission (2004) concluded that the attacks revealed a failure of imagination—stating that "it is therefore crucial to find a way of routinizing, even bureaucratizing, the exercise of imagination." Much effort is being expended by the cybersecurity community to proactively anticipate the most devastating vectors for cyberattacks. Government agencies are particularly concerned about cyberattacks on the 16 critical infrastructure sectors, described earlier in this chapter. Attacks on these sectors would cause considerable hardships for U.S citizens, and would create significant spillover effects to multiple sectors of the U.S. economy. Of these 16 sectors, we focus in detail on the financial services and energy sectors—more specifically, on the power grid. These sectors are the most internally interconnected and interdependent with other sectors as well as most robustly connected to the Web, and are thus at risk for a devastating cyberattacks that would ripple through the entire economy. In this section, we describe the current concerns and ongoing efforts to secure these sectors.

The Financial Sector

Attacks on the financial sector can reduce confidence in the financial system and affect a great number of public and private entities, which rely on the smooth functioning of financial markets and global payment systems for the supply of capital and the transfer of funds. In recent years, certain aspects of the global financial system have proven to be vulnerable to cyber threats. For example, the Bank of Bangladesh reported that over $81 million had been stolen from its account at the Federal Reserve Bank of New York, and more than half the stock exchanges worldwide have reported experiencing breaches and attacks (Anand 2017; Lema 2017). Moreover, in 2011 and 2012, 46 American entities, primarily in the U.S. financial sector, faced DDoS attacks by Iranian individuals in Iran-based computer companies that conducted work "on behalf of the Iranian Government." The attacks resulted in as much as 140 gigabits of data per second and hundreds of thousands of customers preventing from online access to their bank accounts (DOJ 2016b).

A number of attempts have been made to exploit vulnerabilities in cybersecurity infrastructure in order to create desired movements in stock prices. To be clear, an attack does not need to target the financial sector to have financial market effects. The majority of these incidences have been small in scale and directed at specific companies. For example, in 2015 actors posted a fraudulent story that Twitter was in talks to be acquired for $31 billion. This story, posted on a website designed to mirror Bloomberg, drove Twitter's share prices up by over 8 percent before further investigation revealed that the story and website were fraudulent.

False news reporting has also moved the broader market. In 2013, members of the Syrian Electronic Army gained access to the Associated Press's official Twitter account, and subsequently tweeted that the President had been injured in two explosions targeting the White House. This tweet caused the Standard & Poor's 500 Index alone to lose $136.5 billion in market capitalization; however within 6 minutes, the losses were erased when the Associated Press and other sources noted that the tweet was a hoax (Domm 2017). The three members of the Syrian Electronic Army were ultimately charged with multiple conspiracies related to computer hacking by the Department of Justice (DOJ 2016a), with the hack of the Associated Press's Twitter account used as evidence.

Cyberattacks on the financial sector could impose substantial costs on the U.S. economy. If investors could no longer trust that traded securities were priced efficiently, financial assets would lose their attractiveness as investment vehicles. In turn, firms would no longer be able to rely on the stock market as a reliable means for raising capital. As a result, the cost of capital would increase, reducing economic growth. Investors, having moved into other investment assets, would likely incur higher costs associated with information gathering,

and would lose the benefits associated with liquidity and risk sharing facilitated by well-functioning financial markets.

The Defense Advanced Research Projects Agency (DARPA 2017), a part of the U.S. Department of Defense, runs a pilot program to identify and help mitigate the risks to the financial sector that could be posed by cyber threat actors. So far, DARPA has identified several areas of concern. Among them is the risk of so-called flash crashes, named after the 2010 Flash Crash. To achieve flash crashes, sell orders can be manipulated to cause a rapid decline in the stock market index. Though the mispricing corrects quickly, it creates economic costs for market participants, because wealth is being redistributed across traders in an arbitrary manner, and it causes investors to lose trust in the stock market. If flash crashes become a frequent occurrence, high-frequency traders could be forced to exit the market, potentially leading to lower liquidity levels.

Another area of concern is an attack on the order-matching system, which would cause a random fraction of trades to be left unmatched and would result in unwanted exposures to risk factors that the trader tried to hedge with a combination of long and short positions in securities. Manipulations of data feeds and news feeds, on which the automated trading systems employed by institutional traders frequently rely without human input, could pose another set of challenges to price efficiency. If the intrusions in the data feeds were small in scale and in scope, they would make it difficult to verify the starting and ending times of an intrusion in order to eventually certify that the data feeds are no longer contaminated. DARPA's efforts focus, among other things, on constructing simulated trading environments and then attacking these environments with various attack vectors in order to evaluate which defense solutions work best.

The Power Grid

A cyberattack on the power grid could have devastating consequences for firms and private citizens. Lloyd's of London and the University of Cambridge's Centre for Risk Studies lay out a scenario for how hackers could attack power grids with malware that could lead to large-scale blackouts in the United States. At the basis of this scenario are real-world examples of attacks on power grids (Lloyd's of London 2015). Such examples include the December 2015 and 2016 attacks that cut power in Ukraine. Cybersecurity companies involved in the investigation of the Ukraine attack found a piece of software capable of ordering industrial computers to shut down electricity transmission (Reuters 2017a). As electrical systems become more intelligent, they become an easier target for cyberattacks and data breaches.

A cyberattack on the electrical grid would have large-scale economic effects, because infrastructure damage, loss of output, delayed production, spoiled inventory, and loss of wages all decrease productivity and earnings for the duration of the blackout. In addition to the economic effects of a

large-scale power outage, there are concerns related to health and safety and national security. DARPA is performing a large-scale study of how to best prevent and mitigate cyberattacks on the power grid. Among other things, DARPA is building grids that are isolated from the power grid network, and it is using various attack vectors and other methods of defense to determine the most effective form of defense against possible cyberattack scenarios.

A cyberattack launched against the electric grid could affect large swaths of the U.S. economy, because most economic activity is dependent on access to electricity. Economic analysis conducted by various industry studies estimates that cyberattacks against critical infrastructure assets could cause up to $1 trillion in damage (Tofan 2016; Lloyd's of London 2015, 2017). The tail risk scenarios described in this section indicate that cyberattacks on critical infrastructure sectors could result in escalating cyber costs that eclipse the ongoing costs of doing business in an interconnected world.

The Rise of Quantum Computing and the Need for Better Encryption

A final potential threat to the existing cyber infrastructure is the rise of quantum computing and the possibility that a malicious actor may have access to a powerful quantum computer. Cybersecurity depends to a large extent on public key encryption technologies, such as the widely used algorithm named RSA. With RSA encryption, a message is encoded using a public key, and then decoded using a key known only to the private user. The connection between the two keys often is a complicated and time consuming math problem, such as prime number factorization, which could in principle be solved, but may take hundreds or even thousands of years of computing time to do so.

A traditional digital computer relies on bits, which can take on a value of 0 or 1. Newly developed quantum computers instead rely on quantum bits, or "qubits," that are not constrained to a binary nature. A quantum computer can take advantage of the possibility that a quantum variable, such as the spin of an electron, can probabilistically occupy more than one state simultaneously (i.e., be both 1 and 0 at the same time). Different particles can have states that are correlated with one another, allowing small numbers of correlated quantum bits to express distributions that would require far more normal bits to express. In some cases, algorithms, such as that introduced by Shor (1997), have been developed that utilize these processes to allow the computer qubits to multitask. This increased processing efficiency could allow quantum computers to develop solutions to problems in much less time than would be necessary for a traditional computer.

A world with quantum computing would not necessarily be less secure than today's world. Cryptographies that rely on alternative approaches such as lattices, multivariate polynomial equations, or even those that use current

approaches but rely on larger prime factorizations may well be secure in the quantum computing world.

The problem lies in the transition to that world. If quantum computing advances faster than anticipated, a large amount of data could be incorrectly believed to be secure, when in fact it is not. A malicious agent who moves the fastest in this space could potentially subject the economy to large-scale security breach. Moreover, the agents who anticipate the eventual emergence of powerful cyber computers that can decrypt currently safe files may have an incentive to steal and archive today's encrypted files so they can be decrypted in the future. Things that are safe today may not be in retrospect, which raises a host of pecuniary and nonpecuniary concerns. Thus, the economic costs of cyberattacks and data breaches may well increase sharply relative to our current estimates if malicious actors gain an upper hand during the transition period.

Given such costs, cybersecurity will continue to be a high-priority national-security issue for many years to come. The private sector and the U.S. government have a number of ongoing efforts to reduce the cyber risk. We describe these efforts next.

Approaches to Reducing Cyber Risk

Defending against cyber threats requires building effective and evolving cybersecurity capabilities that span all entities in the U.S. economy, and no single solution is expected to permanently resolve the cyber problem. Current efforts across the public and private sectors to address cyber concerns are already under way. They are a step in the right direction, but the ever-evolving nature and scope of cyber threats require continued efforts. Effective cyber protection will require the cooperation of the private and public sectors to report and mitigate cyber threats.

Public Sector Efforts

As discussed earlier in the chapter, cybersecurity is a common good, and therefore government involvement in cybersecurity efforts may be beneficial. The U.S. government is actively facilitating cybersecurity solutions on multiple fronts. Because no single private entity faces the full costs of the adverse cyber events, the government can step in to achieve the optimal level of cybersecurity, either through direct involvement in cybersecurity or by incentivizing private firms to increase cyber protection. When the adversary is as formidable as a nation-state, the government may be the only defender with the adequate resources and technology to meet this challenge. Additionally, as a frequent target of attack, the government sector is already actively involved in cyber protection. For example, one of the tasks of the Department of Homeland Security is to protect the dot-gov domain (U.S. Congress 2017b), and a number

of other government agencies are tasked with protecting various critical infrastructure sectors against cyber threats. Because the government is able to achieve economies of scale in its responses to cyber threats, it is cost-efficient for the government to take an active role in aggregating information, monitoring cyber threats, engaging in defensive action, disseminating knowledge, and devising effective policies.

Information sharing and transparency. Information sharing is crucial for coordinating cybersecurity efforts, informing public and private entities of cyber vulnerabilities, determining appropriate levels of defense investments, and facilitating the effective functioning of the cyber insurance market. However, private sector firms face a strong disincentive to voluntarily disclose cyber vulnerabilities because of business and reputational concerns. To overcome these dynamics in the market, the government may facilitate information sharing through a variety of channels. For example, government-monitored information-sharing platforms for anonymous disclosures of adverse cyber events are designed to increase the real-time awareness of cyber vulnerabilities and facilitate timely and publicly shared security solutions. The Automated Indicator Sharing (AIS) Program at DHS (2016a) facilitates the sharing of "commercial data feeds, internally generated analytic products, analytics tools, threat indicators and warnings, real time incident, and continuous monitoring data." Additionally, the FBI issues Joint Indicator Bulletins, Joint Analysis Reports, Private Industry Notifications, and FBI Liaison Alert System (FLASH) reports that inform public and private entities about cyber threats (FBI 2017c). Other mechanisms to increase transparency about cybersecurity breaches that were discussed earlier in the chapter are the SEC's 2011 Guidance, the HIPPA disclosure requirements and the Department of Energy's OE-417 Electric Emergency Incident and Disturbance Report. U.S. Congress has also proposed legislation on cybersecurity disclosure; for example, the Cybersecurity Disclosure Act of 2017 (proposed by the Senate Committee on Banking, Housing, and Urban Affairs), which seeks to ensure disclosure on cybersecurity expertise and measures taken by qualifying firms (U.S. Congress 2017a).

Cyber protection investments. Basic research on cybersecurity generally underlies investment in cybersecurity. Though this research may benefit from economies of scale if data and resources are pooled across organizations, companies generally do not have incentives to share this basic research with each other, and this may result in duplicative investment efforts across companies. Therefore, direct government investment in this research may be a way to leverage economies of scale that ultimately benefit private firms across industries. Firms may then take the responsibility to adapt this research to the needs and risks of the companies in question. Also, it is often argued that market forces provide firms with little incentive to invest in basic research because the nontrivial nature of knowledge makes it difficult for firms to appropriate the resulting returns. Government support for basic research can overcome

the lack of incentives and generate critical discoveries that will benefit society writ large.

Indeed, the Federal government has made investments in cybersecurity basic research and threat analysis, particularly through DARPA. In fiscal year 2018, DARPA's budget allocated about 10 percent ($41.2 million) to research in the cyber sciences, most of which went to the Transparent Computing program, which seeks to create technologies that will allow for better security policies in distributed systems, such as distributed surveillance systems, autonomous systems, and enterprise information systems (DARPA 2017). Such government investment in basic cyber research benefits from economies and scale and may reduce private firms' duplication of research efforts. For example, DARPA's basic research investments in unmanned aerial vehicles have spurred innovation in the private aerospace industry (DARPA 2015). According to the Office of Budget and Management, Federal IT spending, which includes cybersecurity, has been on an upward trajectory since 2013 (OMB 2017).

The public sector may also incentivize private sector investment in cybersecurity firms to increase the availability and growth of cybersecurity products and services. For example, Maryland's government provides a refundable income tax credit to qualified Maryland cybersecurity companies. These companies receive a credit of 33 percent of an eligible investment, though the credit is limited to $250,000 for each investor during each fiscal year (Maryland Department of Commerce 2017).

Cybersecurity standards. Standards for cybersecurity are also important ways to ensure that companies are aware of proper cyber practices. Standards are effective to the extent that they enable a risk-based approach to cybersecurity, which naturally varies across sectors and firms. For example, such cybersecurity standards may create a common lexicon for cybersecurity, including the definition of what constitutes a cyberattack or a data breach, which currently is not standardized across government and private organizations. The 2013 U.S. Executive Order 13636 "Improving Critical Infrastructure Cybersecurity" encourages the U.S. government's IT agencies to adopt "The Framework for Improving Critical Infrastructure Cybersecurity," as developed by NIST, in order to enhance risk management. For example, the Financial Services Sector Coordinated Council (FSSCC 2017), which seeks to "strengthen the resilience of the financial services sector against attacks and other threats," in collaboration with the Department of Treasury, has developed an automated cybersecurity assessment tool. Though standards can be beneficial for addressing cyber threats, if they are not properly coordinated across government agencies and are too prescriptive, they could be very costly to implement and thus lead companies to use a compliance-based rather than risk-based cybersecurity approach.

The NIST cybersecurity framework is an example of a standards tool that was originally targeted for critical infrastructure, then adopted by the broader

government community (both inside and outside the United States, e.g., in Italy), and increasingly by the private sector (NIST 2017b). It is a voluntary, broad-based set of standards that seeks to "identify effects of cybersecurity on business; align and de-conflict cybersecurity requirements; prioritize cybersecurity outcomes; organize, authorize, task and track work; express risk disposition; and understand gaps between current and target." The framework is made up of five functions: to identify, protect, detect, respond, and recover from cyber risks. It also establishes a common lexicon to discuss cybersecurity issues across stakeholders, and it is meant to be adaptable to changing cyber technologies and threats. All 16 critical infrastructure sectors adopted NIST's cybersecurity framework in fiscal year 2016 (U.S. Department of Commerce 2017; NIST 2017a).

Industry-wide cybersecurity standards may also ensure the security of supply chains by providing a baseline of risk management and other security mechanisms across firms. NIST has established standards for a risk management process to ensure the cybersecurity of supply chains, known as the Cyber Supply Chain Risk Management process (NIST 2018).

International efforts. Cyber risks may also result from foreign government actions or weak cyber defenses across countries, which may be addressed through international diplomatic and enforcements efforts. For example, the United States initiated the "Section 301 Investigation of China," pursuant to the Trade Act of 1974, to assess Chinese practices, including cyber practices, which may weigh on U.S. commerce. Also, the United States annually discusses problematic cyber practices that could put IP property in the country at risk and affect U.S. commerce in the annual Special 301 reports. The World Trade Organization's Agreement on Trade-Related Aspects of Intellectual Property Rights (known as TRIPS) could also be a tool for addressing unfair cyber practices abroad; however, at this point, it seems to be primarily focused on other, non-cyber-related forms of IP theft. International bodies—such as the G-7, G-20, and Financial Stability Board—have also provided forums to address cybersecurity issues in the financial sector. For example, in October 2017, the G-7 adopted the "Fundamental Elements of Cybersecurity for the Financial Sector" which sets "non-binding, high-level fundamental elements" for private and public actors in the financial sector to customize to their specific regulatory landscapes and cyber risks (Department of Treasury 2017). In the same year, G-20 Finance Ministers and Central Bank Governors released the "Roadmap for Digitalization: Policies for a Digital Future," which included a provision to "strengthen trust in the digital economy," including through "exchanging experiences" on "guidelines and best practices to identify, assess, and manage security risks" (German Federal Ministry for Economic Affairs and Energy 2017). Finally, the international Financial Stability Board has facilitated communication between international public and private sector actors on cybersecurity in the financial sector (FSB 2017).

Governments can also pursue bilateral measures. For example, in September 2015 the U.S. and China signed the nonbinding Cyber Agreement (referred to as the Xi Agreement), whereby the two countries agreed to (1) "timely responses" regarding "malicious" cyber activities; (2) cooperation on cybercrime investigations, and provision of updates, "consistent with their respective national laws and relevant international obligations"; (3) ensuring that neither government would "conduct or knowledge support" cyber-enabled theft of IP, including "trade secrets or other confidential business information for commercial advantage"; (4) promoting norms for nation-states' cyber behavior within the international community; and (5) creating a high-level joint dialogue to "fight" cybercrime and related issues (White House 2015; CRS 2015). It has been noted that the number of suspected network compromises by 72 China-based groups in the U.S. and in 25 other countries has declined since mid-2014, since the Xi agreement, from a peak of over 70 compromises in August 2013 to fewer than 5 in May 2016.[9] In his 2017 Worldwide Threat Assessment, the Director of National Intelligence confirmed that the volume of cybercrimes committed by China has declined since the September 2015 commitments, but noted that China continues to actively target U.S. firms and government for cyber espionage (DNI 2017).

Developing a cybersecurity workforce. There is a significant skills gap in the cybersecurity field, which is reflected in a shortage in the number of American workers left to fill cyber positions. Almost 210,000 cybersecurity jobs went unfilled in the United States in 2015 alone (McAfee 2016). Projections estimate that the global shortage will increase to 1.5 million unfilled positions by 2020.

Cybersecurity jobs are a subset of IT jobs; however, the number of cyber job occupations is expected to grow by 28 percent between 2016 and 2026, "much faster than the average for all occupations." In comparison, the growth rate for all computer-related jobs is projected to be 13 percent, while the growth rate for all other occupations is projected to be only 7 percent during this same period (BLS 2017).

One possible source of the cybersecurity workforce shortage is that access is lacking to education in science, technology, engineering, and mathematics (STEM), and particularly to computer science (CS)—a field within which cybersecurity falls—for schools from kindergarten through grade 12. For example, more than half these schools do not offer computer programming coursework (Gallup 2016; Code.org 2016), and almost 40 percent of high

[9] The 25 other countries and economies, in order of the frequency of incidents, are the United Kingdom, Japan, Canada, Italy, Switzerland, Germany, the Netherlands, India, Australia, Denmark, Philippines, Sweden, Taiwan, Brazil, China, Colombia, Colombia, Egypt, France, the Hong Kong Special Administrative Region, Israel, South Korea, Norway, Saudi Arabia, Singapore, and Tunisia. Of the 262 compromises that occurred during the 2013–14 period, 182 (69.5 percent) occurred on U.S. entities' networks, and 80 (30.5 percent) occurred on networks in the other 25 countries.

schools do not offer physics (U.S. Department of Education 2016). Greater access to STEM and CS programs for younger students would likely increase the number choosing to pursue these fields at a higher level. This is especially important for the cybersecurity labor force, given that many of the available cyber positions require significant educational credentials and experience. About 84 percent of cybersecurity postings require a bachelor's degree at a minimum, and 83 percent ask for at least three years of previous experience (Burning Glass Technologies 2015). Meanwhile, almost 79 percent of students in the United States pursuing a master's degree in CS are citizens of other countries (NFAP 2017).

These numbers indicate a dependence on foreign workers and foreign companies to help meet much of the United States' domestic cybersecurity needs. An example portraying the necessity of decreasing our dependence on foreign cybersecurity expertise is the case of Kaspersky Lab, a prominent Russian cybersecurity research firm founded in 1997 and headquartered in Moscow (Subcommittee on Oversight 2017). Kaspersky's antivirus software has been sold throughout the United States, and was even being used in the computer systems of some two dozen Federal agencies. As with most security software, Kaspersky's antivirus products require access to everything stored on a computer, which allows it to search for viruses or other malware. By conducting scans for malicious software, the program removes any risks and sends back a report to the company. Though this is a routine procedure, in 2017, suspicion grew that the software was in fact providing an all-too-perfect tool for Russian intelligence to access content of interest on American computers, especially those utilized by the government.

DHS issued a directive on September 13, 2017, for Federal Executive Brand departments and agencies ordering them to remove and discontinue use of Kaspersky products (DHS 2017c). In the press release DHS stated that "the risk that the Russian government, whether acting on its own or in collaboration with Kaspersky, could capitalize on access provided by Kaspersky products to compromise Federal information and information systems directly implicates U.S. national security." The case of Kaspersky demonstrates the critical need to increase the domestic supply of cyber workers, and reduce American dependence on foreign cyber products, which cannot always be trusted, and instead develop our own cyber expertise.

Meanwhile, another source for the cyber workforce shortage is the lack of diversity in the field, particularly the underrepresentation of women. The share of CS degrees awarded to women by higher education institutions has fallen over the past 30 years. In 1985, the proportion of women earning CS degrees for all levels of education was approximately 36 percent. By 2015, this share had dropped to about 22 percent (NCES 2016). The reasons for the decline in female CS degree enrollment are not well understood, though there are a number of

competing explanations (e.g., Roberts 1999; Irani, Kassianidou, and Roberts 2002; Wang et al. 2015).

Corresponding to the low percentage of women studying CS, the share of women in CS occupations was only 24.5 percent in 2015 (NSF 2017), well below the rate of 34 percent in 1990 (U.S. Census Bureau 2013). For comparison, in 1990 women represented 45 percent of the labor force, compared with 47 percent in 2015 (DOL 2017). For cybersecurity positions specifically, which typically require a CS background, a 2017 study conducted by the Center for Cyber Safety and Education found that the number of women working in the cybersecurity field in the United States is a mere 14 percent. Other studies suggest that women make up as little as 10 percent of the U.S. cybersecurity labor force. Increasing the domestic cybersecurity workforce will crucially rely on attracting more U.S. women to CS coursework—and thus to the cybersecurity profession.

Although many technology companies already offer STEM-related scholarships to women, the government should continue to promote grants offered to women studying CS (and cybersecurity) through various avenues, such as the National Science Foundation. It is equally important to provide female-to-female mentoring to help encourage women to study CS. By offering structured opportunities for mentorship, women can better understand the field while interacting with female leaders and role models (Bohnet 2016).

Additionally, universities need to consider the impact of professors' genders on the gender gap in the sciences (Carrell, Page, and West 2010; Vilner and Zur 2006). Though a professor's gender has little effect on male students, it can play an important role in the performance of female students in math and science, and can affect their likelihood of pursuing STEM degrees. Research suggests that the gender gap in academic performance and STEM majors can be eliminated, specifically for high-performing female students, when introductory math and science courses are taught by women.

Overall, the Administration is playing a leading role in the STEM movement, attracting both women and men to the cyber field by offering more opportunities for exposure to STEM concepts earlier in life. The Administration is already spearheading a movement to promote greater access to computer science education in elementary and high schools (see White House 2017a), directing the Department of Education to invest at least $200 million in annual grants to help fund the expansion of STEM and CS in schools across the country. Additionally, Executive Order 13800: "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" aims to foster the "growth and sustainment of a workforce skilled in cybersecurity and related fields" in the public and private sectors, beginning with an assessment of current cybersecurity workforce development programs in the U.S. and in cyber peers.

Raising cybersecurity awareness. Governments may inform consumers of cyber risks to ensure that demand-side factors internalize cybersecurity

risks. For example, governments—at the Federal, State, and local levels—may also educate consumers about cybersecurity, including current vulnerabilities and best practices, to ensure that consumers demand secure products and therefore incentivize businesses to supply such products. For example, DHS initiated the Stop.Think.Connect Campaign to increase public awareness of cyber threats—which includes toolkits customized for students, parents, young professionals, the elderly, government, industry, small business, and law enforcement—discussing topics such as reporting a cybercrime complaint, recognizing and reducing cybersecurity risk, online privacy, and phishing. The campaign also disseminates instructional videos and audio materials on cybersecurity (DHS 2017a).

Protecting critical infrastructure. Cyber protection is particularly important for critical infrastructure, given the potential for both physical and virtual damage to systems that may affect many people and organizations at once—for example, in the case of a disruption in the electricity grid or power plant. The public sector is particularly important in preventing and addressing such breaches because of the magnitude of negative externalities that are possible with such a breach. In line with this, Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," seeks to strengthen cybersecurity risk management in critical infrastructure sectors.

Several executive orders over the last several years have addressed protection and coordination concerns about critical infrastructure cyber networks. The 2013 Presidential Policy Directive-21 (PPD-21), "Critical Infrastructure Security and Resilience," notes the above-mentioned 16 critical infrastructure sectors that are important for both the U.S. economy and national security, for which cyber protection is particularly essential. That same year, Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," expanded the Enhanced Cybersecurity Services program that enables real-time sharing of cyber threat information, and ordered NIST to develop a cybersecurity framework. Most recently, in May 2017, Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," includes efforts to improve cybersecurity risk management across the government (White House 2017b). It is too early to assess the effectiveness of these orders, but their implementation is an important step toward limiting cyber risks.

Law enforcement in cyberspace. Effective law enforcement is critical for discouraging cybercrime, and its continued success is predicated on coordination among various law enforcement agencies. The FBI Cyber Shield Alliance, initiated by the FBI's Cyber Division, engages in partnerships with U.S. State, local, territorial, and tribal law enforcement agencies to synchronize efforts against cybercrime. Law enforcement agencies and private entities may report cyber incidents through the FBI's online portal system.

Law enforcement has had major successes bringing charges against criminals in cyber space and helping dismantle their criminal operations,

Box 7-9. Law Enforcement's Role in Mitigating Cyber Threats: The Kelihos Botnet

The Kelihos botnet was a malicious operation that started in 2010 as a global network of tens of thousands of infected computers running on Microsoft's Windows operating system (DOJ 2017a). The botnet was used to steal the login credentials of infected users and send hundreds of millions of spam emails that included malicious software and ransomware (DOJ 2017a). At its peak, the botnet grew to over 100,000 infected computers, ordering them to carry out various cybercrimes including password theft, pump-and-dump stock schemes, and the advertisement of counterfeit drugs.

The DOJ led the effort to free the infected computers from the botnet (DOJ 2017a). Specifically, the DOJ obtained warrants under Rule 41 of the Federal Rules of Criminal Procedure, allowing it to establish substitute servers into which to redirect Kelihos-infected computers, and also to collect the Internet Protocol addresses of the computers that connected to the servers (DOJ 2017a). This was done to provide these addresses to those who can assist victims in removing the malicious software from their computers (DOJ 2017a). And this operation also blocked all commands sent in an attempt to regain control of the victimized computers.

The DOJ, in partnership with a private security firm who provided technical analysis and aid, provided the legal means necessary for successful execution. In addition to liberating the already infected devices, the DOJ pledged to continue to share samples of the Kelihos software with all the major players in the cybersecurity industry, thereby training the antivirus software to detect and remove the botnet, should it resurface (DOJ 2017a). Microsoft's Safety Scanner is one example of an antivirus software now programmed to do this, thanks to the efforts of the DOJ.

including many that were located abroad. For example, in April 2017, DOJ played an active role in disrupting the Kelihos botnet and later extradited him to the U.S. This operation is described in detail in box 7-9. This and other successful operations demonstrate the important role of law enforcement in reducing cyber threats and discouraging future cybercrime.

Private Sector Efforts

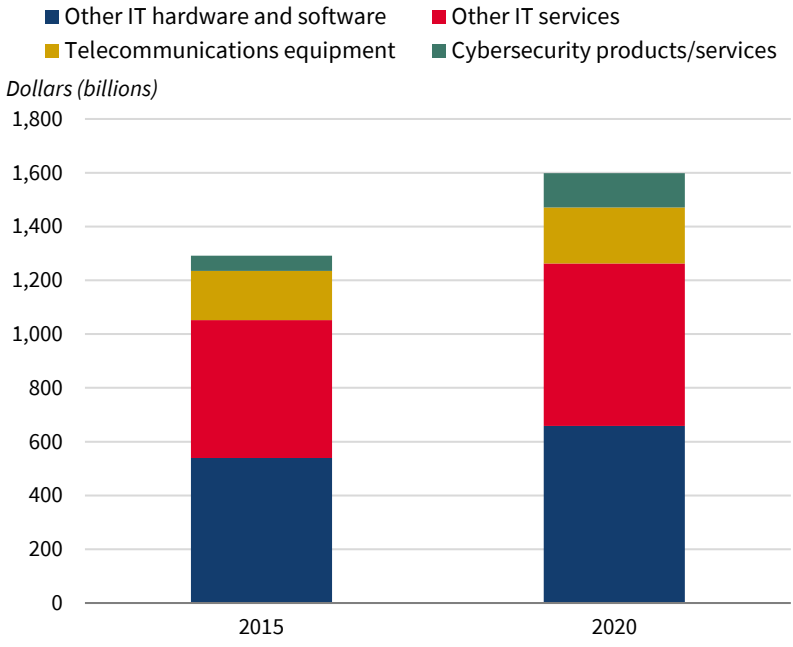
Although the government can help address some elements of cyber protection, ultimately, the most direct cybersecurity actions are in the hands of the private sector. These include direct investments in cyber protection, emergency preparedness, and information sharing, among others. Together, these efforts strengthen a firm's ability to prevent, address, and recover from security breaches.

Investments in cyber protection. Although the public sector may have a comparative advantage in basic research that depends on economies of scale, cyber risks for particular industry-specific factors are most efficiently addressed by private firms because they own and operate most critical infrastructure. One indicator of cybersecurity investment is venture capital funding for and major industry spending on services from cybersecurity firms. This funding has recently more than doubled, from $108 billion in 2010 to $336 billion in 2015 (Nasdaq 2016). And Morgan Stanley (2016) estimates that spending on cybersecurity products and services will again more than double, from $56 billion in 2015 to $128 billion in 2020, though spending on these products will remain below spending on other IT hardware, software, equipment, and services (figure 7-7). Moore (2016) notes that in a survey of 40 executives, mostly at the level of chief information security officer, most respondents (88 percent) reported that their cybersecurity budgets have increased. The survey revealed that frameworks, compliance obligations, and direct engagement with business units on cyber threats were common ways for executives to gain greater budgets for cybersecurity. The survey noted that the most frequently cited response for investment was "perceived risk reduction," followed by compliance and industry best practices.

Private investments in cyber protection can come in the form of cyber services and technologies. At the service end, Ernst & Young (EY 2014) emphasizes the importance of strong security operations centers, aligned with business concerns, that stay informed about impending threats. Such a center could embody a "cyber threat intelligence capability" addressing questions such as "What is happening out there that the organization can learn from [the experience]? How can organizations become "target hardened," and is this required? How are other organizations dealing with specific threats and attacks? How can the organization help others deal with these threats and attacks? Which threat actors are relevant?" (EY 2014). According to EY's survey, 36 percent of respondents attested to not having a threat intelligence program, suggesting that some companies either perceive low cyber threats or are underfunding cybersecurity.

There are also a variety of security technologies that may be used to reduce exposure to cybersecurity risk. Ponemon (2017a) notes that the most common ones in its sample of 254 companies are security intelligence systems (67 percent), which also have the highest reported costs savings and returns on investments ($2.8 million and 21.5 percent, respectively); these are followed by advanced identity and access governance, advanced perimeter controls, extensive use of data loss prevention, and deployment of encryption technologies, among others (figure 7-8). Morgan Stanley (2016) projects that companies will move away from "a la carte solutions" to "more-efficient platforms," resulting in greater consolidation in the cybersecurity industry, with the five largest

Figure 7-7. Investment Projections in Cybersecurity



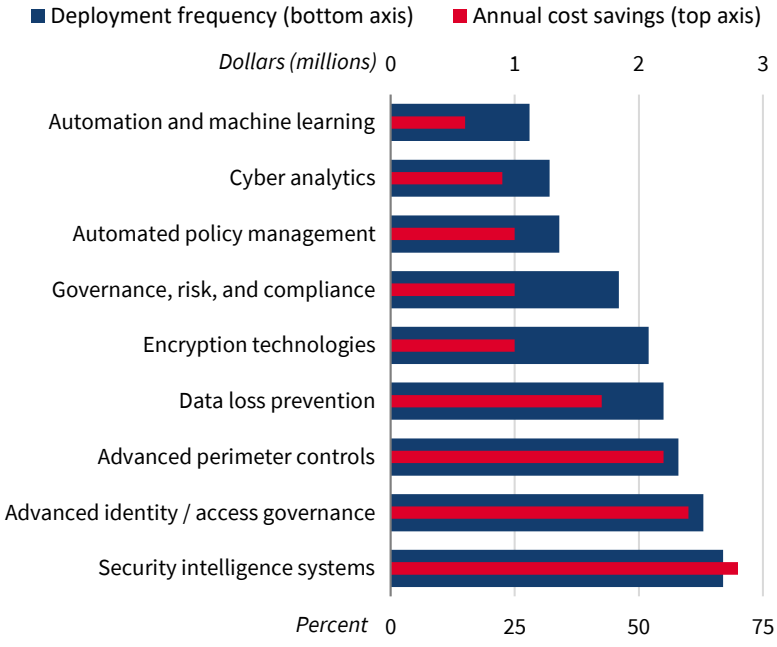
Source: Morgan Stanley (2016).

security vendors growing from 26 percent market share to 40 percent in the short to medium terms.

The use of distributed ledger technology to ensure data integrity. Distributed ledger technology (DLT) is an innovative technology-based solution to address cyber threats and provide data integrity. DLT entails having a database of transactions decentralized across multiple sites in order to eliminate the need for an intermediary to process, validate or authenticate peer-to-peer transactions. Blockchain is a well-known example of DLT that creates a historical record of ledgers that containing every transaction that has taken place among users.

Third-party institutions, such as banks or credit card companies, historically have helped to validate transactions and establish identities. To establish identities, third parties require that users divulge significant, confidential information, which is then stored in a centralized database. As discussed above, centralized PII repositories pose significant risks that the PII data will be stolen by cybercriminals. The additional contribution of DLT to improved cybersecurity is that it is better able than traditional record keeping to ensure data availability and integrity by recording transactions in multiple cryptographically secured public ledgers that are verified in large peer-to-peer networks (Tapscott and Tapscott 2016). The ledgers are distributed around the world

Figure 7-8. Frequency and Cost Savings, by Technology



Sources: Ponemon (2017); CEA calculations.

on computer servers supported by volunteers. Therefore, if any location that holds a copy of the ledger is compromised, other uncompromised ledgers may be used.

Bitcoin is the most popular form of cryptocurrency that uses its own DLT protocol called blockchain. Box 7-10 gives an example of how this technology is implemented.

Better authentication procedures. The relevance and importance of creating and utilizing better authentication methods has intensified in response of the PII incident on Equifax in 2017. Better authentication procedures may prevent cyberattacks and data breaches by ensuring that proper personnel are operating cyber networks. McAfee (2017) notes that "legitimacy tests for every transaction" may identify improper use of network systems. There are other ways of enhancing cybersecurity through authentication improvements. Beyond usage of one-time passwords, individuals and private firms can employ biometrics or two-factor authentication. Two-factor authentication provides an additional layer of security and makes it harder for cybercriminals to gain access to another's account, because knowing the victim's password alone is not enough to pass the authentication check.

In addition, biometric authentication (e.g., using fingerprints or retina scanners) could enhance security as verification is determined by an individual's unique characteristics that are extremely difficult to fake. Network

Box 7-10. Bitcoin

Bitcoin is a piece of open source software that allows for the creation of a secure public ledger of transactions that keeps track of how much bitcoin (the unit of account on the ledger) different users of the system own. At a very high level, there are two key components that allow the system to function. First, Bitcoin uses public/private key cryptography to ensure that transfers of bitcoin recorded on the ledger have in fact been authorized by the owner of the relevant account (Nakamoto 2008). Second, Bitcoin uses blockchain technology to achieve and record consensus on the order and legitimacy of transactions so as to prevent double spending (Nakamoto 2008). These two mechanisms as implemented through the Bitcoin software seek to allow a secure decentralized peer to peer digital payment system to function.

The key technological advance underlying Bitcoin stems from its ability to achieve consensus in a decentralized system. This occurs through a six-step process that was outlined in the original Bitcoin paper (Nakamoto 2008), and is given here, with additional explanations added in brackets:

1. New transactions are broadcast to all nodes. [Nodes can be thought of as individuals or businesses running the Bitcoin software.]

2. Each node collects new transactions into a block. [A block can be thought of as a collection of transactions.]

3. Each node works on finding a difficult proof-of-work for its block. [The proof-of-work is the solution to a computationally intensive mathematic problem that is generated using information embedded in the last accepted block; see step 6.]

4. When a node finds a proof-of-work, it broadcasts the block to all nodes.

5. Nodes accept the block only if all transactions in it are valid and not already spent. [This involves checking the proof of work, verifying the public/private key cryptography to be sure transactions were authorized by the relevant account holders, and verifying that the sender both previously received the funds and has not already spent them.]

6. Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash. [The hash can be thought of as the solution to the computationally intensive math problem, and by using the solution to the last problem to help generate the next one, blocks are linked together in a chain.]

The process described above creates consensus on a decentralized system and de-incentivizes fraud (such as creating multiple accounts or double-spending) by increasing computationally costs (via the proof-of-work requirement). Specifically, fraud requires consistently providing proofs of work faster than the rest of the network, which in turn requires having a majority of the processing power on the network. Bitcoin incentivizes users to participate in the network and produce the proofs-of-work that make the system secure by rewarding users that produce a proof-of-work for a block on

the blockchain with newly issued bitcoin. As time passes, the system increasingly relies on transaction fees to incentivize computational work. Either way, by incentivizing users to do computational work, and by tying the viability of fraud to the amount of computational work being done on the network, the system makes it extremely difficult for fraud to take place. This in turn creates confidence on the part of users that the system and the ledger of transactions it creates is in fact secure and can be used as a payment system.

The bitcoin protocol specifies that only a finite amount of bitcoin will ever be issued (21 million), a significant proportion of which have already been issued (over 16 million). The inherent scarcity of bitcoin is important as it has helped many people to see bitcoin not only as a unit of account and medium of exchange in the decentralized payment system described above but also as a store hold of value. In fact, many see bitcoin as a potential competitor to gold, whereby it serves as an inflation hedge asset that can also be relied upon in a time of crisis. However, similarly to other investment assets, especially those with short trading histories and unclear valuation models, bitcoin may be vulnerable to price bubbles driven by investor sentiment.

Looking forward, bitcoin faces a number of challenges, some stemming from the underlying technology itself and some from the regulatory environment. On the technological front, the bitcoin protocol over time will have to adapt to allow more transactions to go through the system more quickly and with lower average transaction costs. Many competitor crypto-currencies have sprung up seeking to make technological improvements, and this too poses a risk to bitcoin. Additionally, the work of transaction validation is energy-intensive: Böhme and others (2015) estimate that blockchain proof-of-work calculations require more than 173 megawatts of electricity, equivalent to about $178 million per year at average U.S. residential electricity prices. On the regulatory front, a number of regulatory ambiguities also will need to be addressed and the development of broader market infrastructure such as exchanges and ETFs will be important.

In addition, the potential use of bitcoin for illicit transactions—such as money laundering, terrorist financing, tax evasion, and fraud—raises additional regulatory concerns. Some governments like Japan have taken steps to embrace bitcoin, while others like China have sought to limit its use, while many more have taken a piecemeal approach to regulating the technology by applying existing law to entities engaged in regulated activities like running an exchange. For example, in the United States, bitcoin exchanges have to register with the Financial Crimes enforcement Network (FinCEN) as a money services business. Finally, the digital nature of the underlying technology presents cybersecurity risks for bitcoin (Böhme et al. 2015).

segmentation may also reduce unauthorized access to sensitive information on networks. Multiple authentication methods—such as a second factor using

a hardware token or mobile app, including for vendor access—may help to prevent cyber breaches across the supply chain.

Facilitating information sharing. As mentioned above, information sharing is critical for raising awareness of rising cyber threats and solutions across industries. In addition to government-led efforts, industry-led channels may also enable the dissemination of information across private firms, despite reputation and competitor concerns. These channels have the potential to be particularly relevant in addressing industry-specific risks that broader government-enabled channels may not be able to isolate. For instance, across sectors, there are now industry-led information sharing and analysis centers (ISACs), which "collect, analyze, and disseminate actionable threat information" on cyber threats to their members (National Council of ISACs 2017). ISACs span a variety of sectors—including automotive, aviation, communications, defense industrial base, defense security information exchange, downstream natural gas, electricity, emergency management and response, financial services, healthcare, IT, maritime, multistate, national health, oil and natural gas, real estate, research and education networks, retail cyber intelligence, supply chain, surface transportation, public transportation and over-the-road buses, and water.

In general, ISACs have been an important step in promoting information sharing in the industry, partly overcoming the disincentives to share information on vulnerabilities with competitors. However, there is room for improvement to make the information shared in these units actionable by ensuring that cyber breaches are shared in real time. Complementary to ISACs, though not critical infrastructure sector specific, Information Sharing and Analysis Organizations (ISAOs) are facilitated by DHS pursuant to 2015 Executive Order 13691, "Promoting Private Sector Cybersecurity Information Sharing." They are intended to create "transparent best practices" addressing the needs of all industry groups through an "open-ended public engagement" led by the Standards Organization. ISAOs may share information with ISACs (DHS 2016b).

Emergency preparedness and risk management. Companies may minimize the costs associated with cyberattacks and data breaches by ensuring that their organizations have proper response mechanisms in place to recover from attacks, which requires understanding and managing cyber risks. Risk management assessments are a critical way to determine whether systems are protected against cyber threats, and they allow firms to determine whether their level of investment is proportionate to the cyber threats facing them. A risk-based approach takes a customized account of a firm's specific factors—associated with the supply chain, industry, product, region, and the like—to determine the level of cyber threat. Such an approach differs from what some consider a "compliance-based" approach, which involves only following basic guidelines set by regulators.

Once risks are determined, the next step is to ensure that firms are prepared to address and recover from potential cyber breaches. The Federal government lays out several guidelines that may inform such emergency preparedness, including checking whether systems are infected through security scans, disconnecting devices if problems are found, and reporting incidents. Third-party cybersecurity services may also offer risk and emergency preparation tools—although, ultimately, to be effective such preparedness must happen autonomously at the firm level (FireEye 2017).

Outsourcing cyber protection to domestic cybersecurity firms. Some firms may choose to hire security companies to manage cybersecurity risks, both preventing cyberattacks and data breaches and mitigating successful attacks. For prevention, cybersecurity companies offer risk assessments, red-teaming exercises, mergers-and-acquisition risk assessments, and security program assessments, among others. For detection, cybersecurity firms offer incident response services and compromise assessments (FireEye 2017). Outsourcing cybersecurity may be especially valuable for small firms, which typically cannot afford to hire a security professional on staff.

Employee training. Training for employees may be a useful preventive mechanism—for example, training employees on filtering emails and reporting "phishy" emails, and also deterring shared logins (Verizon 2016). Such types of training may build general awareness of the cybersecurity risks associated with daily tasks, such as password protection and information sharing. The NIST Framework includes "awareness and training" in the cybersecurity framework, which requires ensuring that all users are informed and receive training on cybersecurity risks and that stakeholders all understand their roles and responsibilities—including privileged users and third-party stakeholders, which include suppliers, senior executives, and physical and information security personnel.

Other methods. Another way for private firms to improve cybersecurity is by increasing the cost of cyberattacks and data breaches to deter future attacks. One proposal has been to deploy "honey pots" to attract adversaries and distract them from more valuable assets (McAfee 2017). Monitoring internal networks, devices, and applications also may improve detection and recovery from future attacks; this may be done through account monitoring, audit log monitoring, and network / intrusion detection system monitoring (Verizon 2016).

Conclusion

Cyber threats are likely to remain a reality that has an impact on individuals, firms, and the government. Cooperation across the public and private sectors on cybersecurity is ultimately critical as the economy advances to a new era

of technology. Therefore, comprehensive approaches that pool the resources of the private and public sectors are necessary to address the evolving nature of cyber threats. The public sector may enable the reduction of cyber risks by supporting basic research, overseeing cybersecurity standards, engaging in cyber education and awareness, protecting the critical infrastructure sectors, devising methods to overcome barriers to information sharing, and incentivizing private investment in cybersecurity. Meanwhile, the private sector has a comparative advantage in devising technology-based solutions, information sharing, emergency preparedness, and employee training. Effective cybersecurity solutions will contribute to the growth of the U.S. economy.