The Cost of Malicious Cyber Activity to the U.S. Economy

The Council of Economic Advisers

February 2018

Executive Summary

February 2018

This report examines the substantial economic costs that malicious cyber activity imposes on the U.S. economy. Cyber threats are ever-evolving and may come from sophisticated adversaries. Due to common vulnerabilities, instances of security breaches occur across firms and in patterns that are difficult to anticipate. Importantly, cyberattacks and cyber theft impose externalities that may lead to rational underinvestment in cybersecurity by the private sector relative to the socially optimal level of investment. Firms in critical infrastructure sectors may generate especially large negative spillover effects to the wider economy. Insufficient data may impair cybersecurity efforts. Successful protection against cyber threats requires cooperation across firms and between private and public sectors.

Overall:

- We estimate that malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016.
- Malicious cyber activity directed at private and public entities manifests as denial of service attacks, data and property destruction, business disruption (sometimes for the purpose of collecting ransoms) and theft of proprietary data, intellectual property, and sensitive financial and strategic information.
- Damages from cyberattacks and cyber theft may spill over from the initial target to economically linked firms, thereby magnifying the damage to the economy.
- Firms share common cyber vulnerabilities, causing cyber threats to be correlated across firms. The limited understanding of these common vulnerabilities impedes the development of the cyber insurance market.
- Scarce data and insufficient information sharing impede cybersecurity efforts and slow down the development of the cyber insurance market.
- Cybersecurity is a common good; lax cybersecurity imposes negative externalities on other economic entities and on private citizens. Failure to account for these negative externalities results in underinvestment in cybersecurity by the private sector relative to the socially optimal level of investment.
- Cyberattacks against critical infrastructure sectors could be highly damaging to the U.S. economy.

Introduction

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.[1] 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 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 paper. 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. 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). (Analogously to property rights terminology, a cyberattack destroys property or makes it unavailable for use, and a data breach amounts to property theft.) In this paper, we also refer to cyberattacks and data breaches as "malicious cyber activity," "adverse cyber events," simply as "cyber events," and we sometimes refer to data breaches as "cyber theft." When malicious cyber activity is attributed to criminal groups or when it is directed at private individuals, we also sometimes refer to it as "cybercrime."

[1] This report does not consider the entire range of malicious cyber activity that may be of interest to law enforcement but whose dollar impact is difficult to quantify, such as crimes committed by online predators. See https://www.fbi.gov/investigate/cyber for descriptions of various types of 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). Cyber threat actors fall into six broad groups, each driven by distinct objectives and motivations:

Nation-states: The main actors are Russia, China, Iran, and North Korea, according to 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, per our interviews of cybersecurity experts, 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.

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.[2] They 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.

[2] At times, cybercriminals operate alone.

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 cyber incidents and breaches were caused by outsiders, while 25 percent were performed by internal actors (Verizon 2017). Overall, 18 percent of threat actors were state-affiliated groups, and 51 percent involved organized criminal groups. DNI (2017) notes that Russia, China, Iran, and North Korea, along with terrorists and criminals, are frequent cyber threat actors.

Several government and industry sources highlight China's substantial role in cyber-enabled IP theft, asserting that China's "voracious appetite for information" drives significant hacking activity either from Chinese territory or on behalf of the Chinese government (Geers 2014). For example, Verizon (2013) found that China accounted for 96 percent of economic espionage cases in its annual dataset of data breaches. In May 2013, the Pentagon released its annual report to Congress accusing the Chinese government and military of cyberattacks against U.S. public and private sector networks. In May 2014, the U.S. Department of Justice announced indictments against members of the Chinese military for the cyber breaches involving trade secrets and confidential business information. These breaches impacted several U.S. commercial entities: Westinghouse Electric Company, SolarWorld, United States Steel Corporation, Allegheny Technologies Inc., Alcoa, and the United Steel, Paper and Forestry, Rubber, Manufacturing, Energy, Allied Industrial and Service Workers International Union (DOJ 2014).[3] This was the first time in U.S. history that the U.S. government had charged foreign officials with cyber espionage crimes. FireEye (2016) reports that, although the number of network compromises attributable to China declined since mid-2014, potentially as the result of the U.S. government's efforts to address the problem, China's cyber threat became "more focused, calculated and still successful at compromising corporate networks." Looking forward, DNI (2017) predicts that "Beijing will continue actively targeting the US Government, its allies and US companies for cyber espionage."

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 North America—states that malicious cyber activities by nation-states are the fastest-growing category of malicious cybersecurity incidents. Actors who are conducting malicious cyber activity on behalf of nation-states are among the most technically skilled, and security breaches attributable to nation-states often go unnoticed by firms. Although nation-states have historically sought to steal IP, sensitive financial plans, and strategic information, nation-states are often motivated by retaliation goals, and thus may engage in data and equipment destruction and business disruption (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

[3] *U.S. v. Wang Dong et al*, at 4-8.

billions of dollars (Bossert 2017). Cybersecurity experts like to say that in an act of war or retaliation, the first moves will be made in cyberspace. 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 somehow offended the hacktivists. 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, every firm is a potential target, independent of its age, size, sector, location, or employee composition.

At this time, there is no common lexicon for categorizing malicious cyber activities. Some cybersecurity experts believe that it is helpful to focus on the motive and the 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 activities.

In what follows, we estimate the average cost of an adverse cyber event to a firm and discuss the externalities imposed on the economy by weak cybersecurity and the resulting underinvestment in cybersecurity relative to the socially optimal level. Next, we discuss common vulnerabilities to cyber threats and describe the challenges posed by the lack of centralized data on past cyberattacks and data breaches. We then discuss the costs imposed by cyber threats to the U.S. economy, as well as the tail-risk scenarios for a large-scale conflict in cyber space.

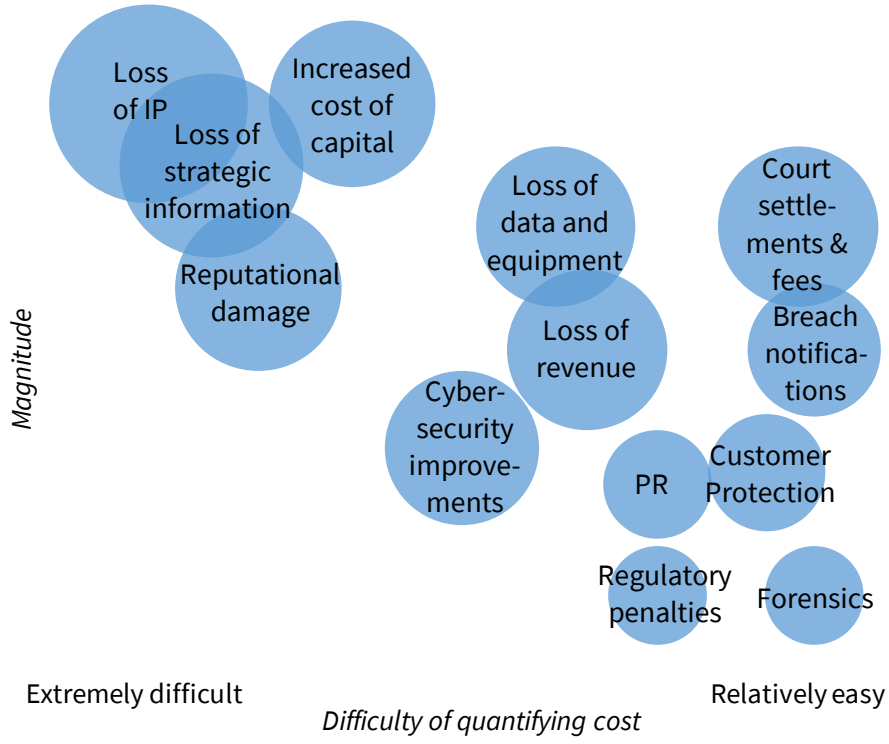
1. The cost of an adverse cyber event for a firm

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.[4] 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 utilizing 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 adverse cyber event, it may face a range of loss categories, some of which are easy to observe and quantify, and some of which are not.

Figure 1 presents a graphical illustration of costs associated with an adverse cyber event, drawing from various sources including the FBI (2017), Verizon (2017), and the Open Web Application Security Project (2014). These costs vary across firms and categories of adverse cyber events. Depending on the nature of their operations, firms are generally exposed to different cyber threats. Consumer-facing 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 to be targeted for IP theft.

Figure 1. Cost Components of an Adverse Cyber Event



[4] In the absence of a centralized data set on cyberattacks and data breaches, many statistics reported in this paper 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 paper, the statistics may be biased down due to underreporting.

Source: McKinsey, CEA calculations.

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 sizeable 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 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 an estimate of how much each cost component contributes to the immediately observable loss and comes up with the following ranks and percent contributions to the total (in parentheses): (1) information loss (43 percent); (2) business disruption (33 percent); (3) revenue losses (21 percent); and (4) equipment damages (3 percent). We must stress that limiting consideration to only immediately observable losses when evaluating the impact of adverse cyber events may drastically underestimate their total cost. This point is illustrated by case studies provided in this document.

A. Estimating the cost of adverse cyber events for U.S. firms

The least subjective method for estimating the impact of a cybersecurity events on a publicly traded firm is to quantify its stock price 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 free 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 on the firm's value. All the expected costs shown in figure 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 at specific firms. The main readerships of the Thomson Reuters newsfeed

are institutional traders and investors, which 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 after. 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 experienced by 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 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 of $15 million is substantially smaller. 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 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. 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 1 presents CARs to the news of adverse cyber events, by sample period.

Table 1. Cumulative Abnormal Returns after News of an Adverse Cyber Event, by Sample Period

Sample Period	Number of obs.	CAR	t-statistic
2000-2013	131	-0.53%	-0.80
2014-Jan 2017	159	-1.01%	-3.42

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.

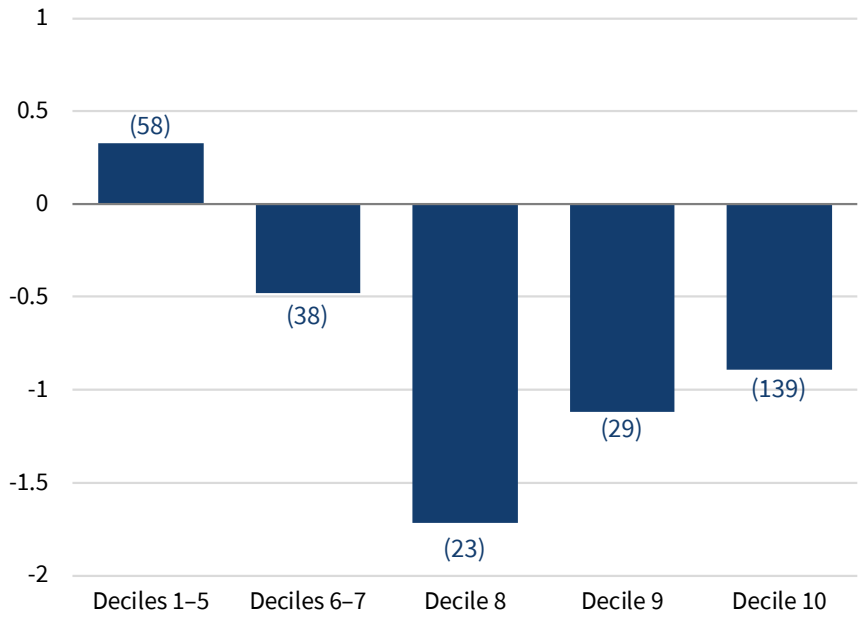
Our study improves on earlier studies with respect to the costs of adverse cyber events because it uses a longer and more complete dataset of such events and estimates the costs from stock price reactions. We obtain markedly more negative estimates of the impact of adverse cyber events on firm values than prior 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 the event. 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 paper—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 2, show a U-shaped relation between firm size and the stock price reaction to the news.

Figure 2. Cumulative Abnormal Return by Size of Firm

(CAR, percent)



Note: Number of observations is in parentheses.
Source: Thomson Reuters; CEA Calculations.

Specifically, figure 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 adverse 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 incidents 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 to mandate 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 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 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 classified them as "nation-states."[5] Of course, nation-states may 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."

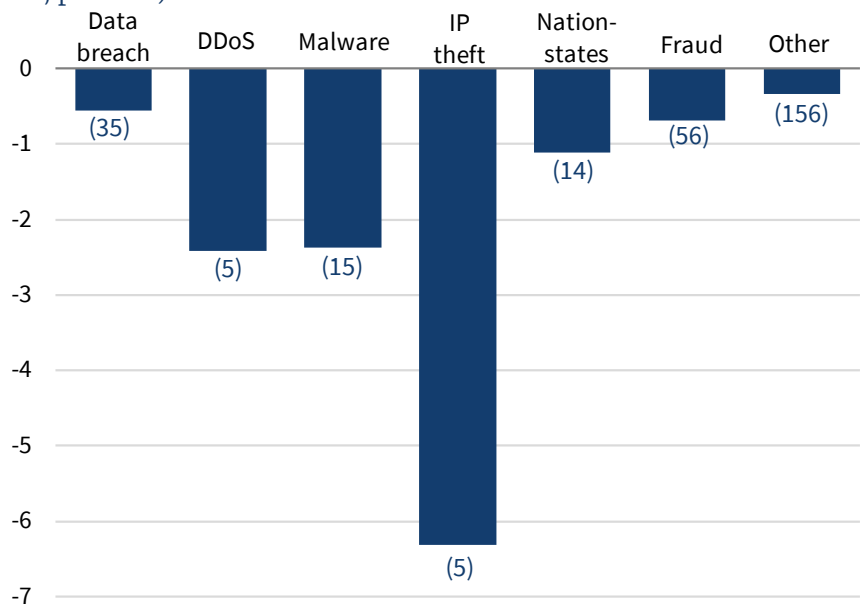
Figure 3 shows the average seven-day CARs associated with the various categories of cyber events in our sample, with the number of observations per each category reported in

[5] 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.

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.

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

(CAR, percent)



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

Although based on a small sample, the figure shows that the market perceives adverse cyber events involving IP theft to be the most damaging, with the victim firms losing, on average, 6.32 percent of their market values. DDoS attacks are a distant second in terms of the damage caused, with the 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, per 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. Attacks 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 attacks is the least damaging on average, with the typical attack 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,[6] 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 convincing (e.g., Mitchell and Stafford (2000) for the description of this econometric approach).[7]

i. 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 exposure 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.

[6] 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.

[7] 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 highly positive. The return on investment in cybersecurity needs to be studied more closely.

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 their 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.

B. Case studies of various types of adverse cyber events.

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 or because the firms were either privately held or listed on a foreign stock exchange. These case studies, as well as other descriptions of cyberattacks and data breaches provided in the text, are based entirely on media reports and our own calculations using public sources, not on 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 descriptions are designed to illustrate that different firms may be targeted for different reasons, and that such adverse cyber events can easily cause substantial material damage to firms.

i. PII data breach.

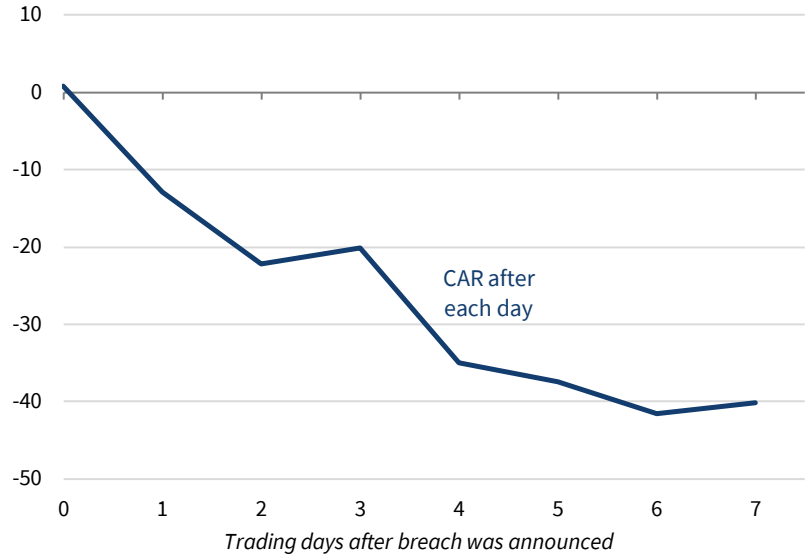
The data breach suffered by Equifax illustrates that a data breach data breach involving PII data can be devastating for a firm if the firm's business model is predicated on mass collection of PII.

Case Study: A Devastating PII Data Breach (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).

Figure 4. Equifax's Cumulative Abnormal Returns After Its Data Breach Announcement

(CAR, percent)



Source: Bloomberg Professional service; CEA Calculations.

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 (Domm 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 4).

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.

ii. Cyberattack by a nation-state

The Sony case illustrates an attack by a nation-state. It is one of the few cyberattacks publicly attributed to a nation-state actor by the U.S. Government.

Case Study: Cyberattack by a Nation-State: Sony Pictures and 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 or data breach. 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 and data breaches on South Korean banks and media outlets, which were carried out by North Korea (FBI 2014). 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 does indicate that the $41 million (Sony 2015) was a damage figure that SPE may have made in March 2015, but even one such article notes as follows: "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).

The Sony attack had adverse effects on the relationship between the United States and North Korea, and it influenced the 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.

iii. IP theft

According to Figure 3, IP theft is the costliest type of malicious cyber activity. Moreover, security breaches that enable IP theft via cyber may go undetected for years, allowing the periodic pilfering of corporate IP. The case below illustrates that IP theft can have a devastating effect on an IP-centered, narrowly-focused firm.[8]

Case Study: Theft of IP and Sensitive Corporate Information by Cyber Means (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 they were dumpling products into U.S. markets 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, and business strategy, and strategy related to the ongoing trade litigation (United States v. Wang Dong 2014).

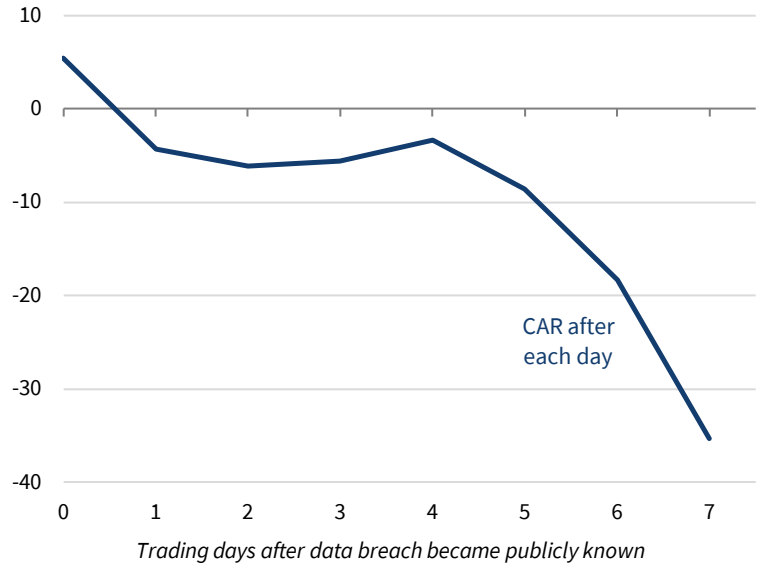
By breaching SolarWorld, Chinese competitors were able to gain access to information that provided them an unfair advantage on multiple fronts (DOJ 2014). A stolen cash flow spreadsheet allows a competitor to know exactly how long SolarWorld would be able to survive a shock. Additionally, production 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

[8] 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 non-cyber means. For example, pirating and counterfeiting of IP-protected products typically involves copying an observed design. According to the 2017 IP Commission Report,

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 5; day 0 in the figure is the day on which the charges were announced), which amounted to a loss of €178 million (CEA calculations).

Figure 5. SolarWorld's Cumulative Abnormal Returns After Its Data Breach Became Publicly Known

(CAR, percent)



Source: Bloomberg Professional service; 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).

C. 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.

The U.S. defines critical infrastructure as systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would

China accounts for 87 percent of counterfeited goods seized coming to the United States. The transfer of IP may be also forced by unfair trade practices, making U.S. firms operating in China particularly vulnerable (USTR 2017b).

have a debilitating impact on national security, national economic security, national public health or safety, or any combination of those matters. The 2013 Presidential Policy Directive-21 (PPD-21), "Critical Infrastructure Security and Resilience," notes that 16 critical infrastructure sectors that are important to both the U.S. economy and national security for which cyber protection is particularly important. 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 U.S. election systems as a subsector of the existing Government Facilities critical infrastructure sector (U.S. Election Assistance Commission (EAC) 2017). PwC (2014) further documents that cyber incidents that involve nation-states were most frequent in the energy, aerospace and defense, technology, and telecommunication sectors. Verizon (2015) estimates that cyber espionage has been increasing in prevalence.

Table 2: Table of Security Incidents and Breaches by Sector, 2016

	Incidents				Breaches			
	Total	Small	Large	Unknown	Total	Small	Large	Unknown
Total	42,068	606	22,273	19,189	1,935	433	278	1,224
Accommodation (72)	215	131	17	67	201	128	12	61
Administrative (56)	42	6	5	31	27	3	3	21
Agriculture (11)	11	1	1	9	1	0	1	0
Construction (23)	6	3	1	2	2	1	0	1
Education (61)	455	37	41	377	73	15	15	43
Entertainment (71)	5,534	7	3	5,524	11	5	3	3
Finance (52)	998	58	97	843	471	39	30	402
Healthcare (62)	458	92	108	258	296	57	68	171
Information (51)	717	57	44	616	113	42	21	50
Management (55)	8	2	3	3	3	2	1	0
Manufacturing (31-33)	620	6	24	590	124	3	11	110
Mining (21)	6	1	1	4	3	0	1	2
Other Services (81)	69	22	5	42	50	14	5	31
Professional (54)	3,016	51	21	2,944	109	37	8	64
Public (92)	21,239	46	20,751	442	239	30	59	150
Real Estate (53)	13	2	0	11	11	2	0	9
Retail (44-45)	326	70	36	220	93	46	14	33
Trade (42)	20	4	10	6	10	3	6	1
Transportation (48-49)	63	5	11	47	14	3	4	7
Utilities (22)	32	2	5	25	16	1	1	14
Unknown	8,220	3	1,089	7,128	68	2	15	51

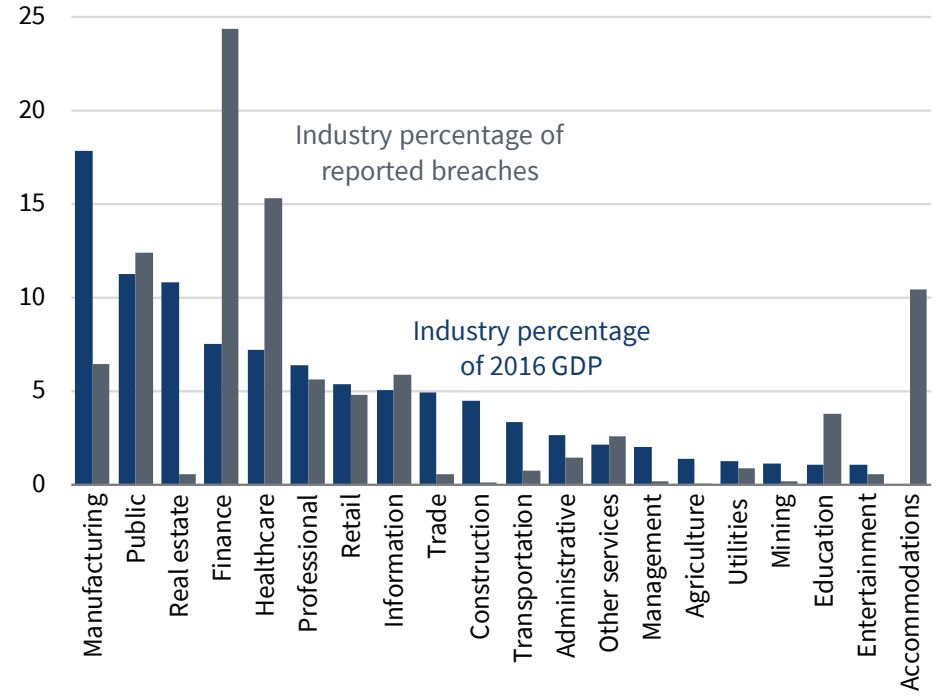
Note: Left columns indicate all security incidents, while the right columns indicate breaches.
Source: Verizon (2017).

According to Verizon (2017), the finance sector, both public and private, saw the most security breaches in 2016, summarized in table 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 (2017) defines large companies as those with more than 1,000 employees, and the rest as small companies.

Figure 6 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.

Figure 6. Distribution of Security Breaches by Industry

(Percentage of 2016 GDP and Breaches)



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

2. 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.

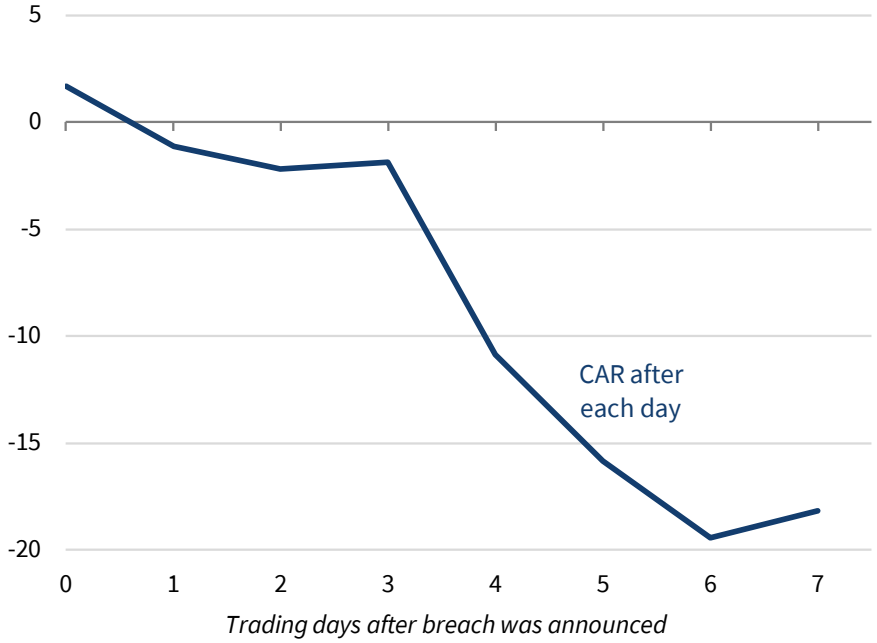
A. Spillovers to economically linked firms

Due to the immense scope of Equifax's data breach and Equifax's centrality in the consumer credit sector of the economy, the data breach caused multiple spillover effects across similar firms and firms tied to Equifax through the supply chain, such as credit card issuing companies. Scherbina and Schlusche (2015) argue that co-mentions in the news media provide information on economic linkages between firms. By performing news searches on Bloomberg and 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.

We identified 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, indicating another potential spillover effect to a cyber breach. 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 ratings 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).

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

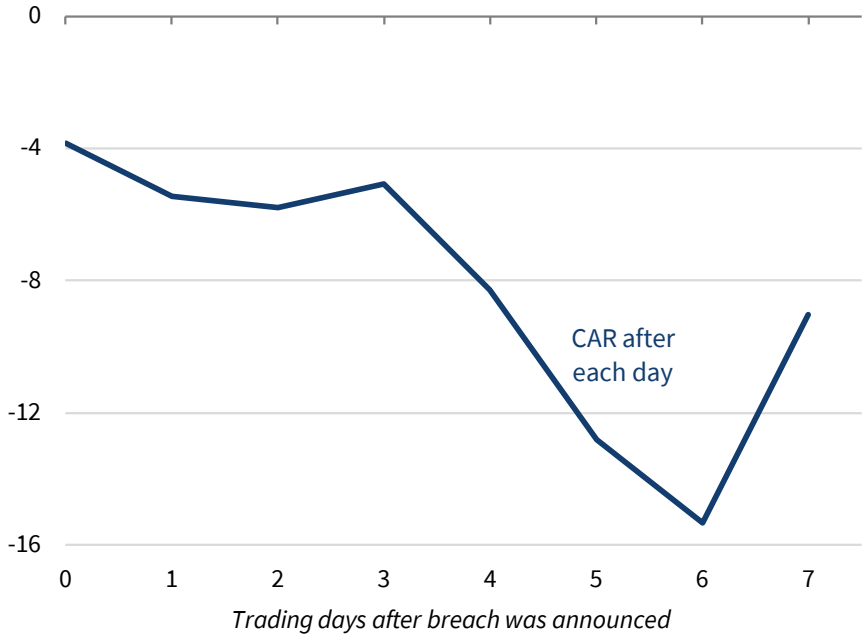
(CAR, percent)



Source: Bloomberg Professional service; CEA Calculations.

Figure 8. Cumulative Abnormal Returns for a Portfolio of Finance Firms After Equifax's Data Breach Announcement

(CAR, percent)



Source: Bloomberg Professional service; CEA Calculations.

We also observed a negative impact of the breach 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 and Company, Synchrony Financial, Fidelity, and Virtu. An equal-weighted portfolio of these firms experienced a negative cumulative abnormal return of over nine percent in the seven day window (Figure 8).

B. 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 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 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.

Case Study: 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.

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 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 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 downstream partners (Patterson Belknap 2017). Additionally, 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).

C. 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 the box blow, is an example of a cybercriminal using an existing security vulnerability to launch an attack against a third party.

Case Study: Exploiting Vulnerabilities to Launch an Attack on 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 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).

D. Economy-wide spillover effects from firms with critical infrastructure assets

Finally, and perhaps most important, if a firm owns a critical infrastructure asset, an attack against this firm could cause major disruption throughout the economy. 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 paper.

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 can 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 cybersecurity measures (see, e.g., Gordon et al. 2015, who conduct an analysis of externalities resulting from weak cybersecurity).

3. 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 weakness. 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 becomes public, it is likely that other firms have experienced the same compromise, even though they may have not 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 the latter later in the section on cyber insurance.

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.

A. 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 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, under the U.S. Department of Commerce, has stated a goal for a "dramatic reduction" in software vulnerabilities. Specifically, the 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.

The Heartbleed vulnerability, described below, illustrates how a security vulnerability in a widely used software has potential to affect multiple firms. Additionally, the case study shows that in some circumstances open-source software may be less secure than commercially produced software.

Case Study: Common Software Vulnerabilities (Heartbleed)

The "Heartbleed" vulnerability affected the OpenSSL library, a widely used open-source implementation of the Transport Layer Security (TLS) protocol in early 2014.

The TLS is one of the standard cryptographic protocols by which systems provide users secure communications over computer networks and the internet. Several versions of the protocol are widely used in applications such as web browsing, email, Internet faxing, instant messaging, and voice-over-IP (VoIP). Websites use TLS to secure communications between servers and web browsers. The open source protocol's user base grew rapidly while the code continued to be maintained by a volunteer group, leading to minimal professional oversight of what came to be a ubiquitous security layer.

In April 2014, it was disclosed that a portion of this security protocol which created secure exchanges between repeat-interaction parties had been compromised. At that time, 17 percent of the certified secure web servers on the web were determined to be vulnerable to this security breach. The Heartbleed attack was ultimately patched rapidly within a seven-day timeframe and saw only a small share (1.5 percent of the top 800,000 websites) affected by the breach.

We now discuss the particularly harmful "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.

i. 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 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 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.

ii. "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, computer system, or 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.

B. Firmware

Firmware comprises 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 cybercrime.

C. Hardware

Hardware is the physical component 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.

As an example, in 2015, a research team at Google was able to achieve a security compromise in several brands of laptops using pre-existing vulnerabilities in the laptops' dynamic random-access memory (DRAM) technology. This compromise allowed for outside actors to change what was stored on the computer's memory without permissions on the system.

An even more striking example of a hardware vulnerability was recently discovered by the Project Zero research team at Google in certain processors manufactured by Intel, AMD, and ARM.[9] Specifically, Google found and reported three unique vulnerabilities useable against these processors to the processors' respective manufacturers on June 1, 2017.[10] Kocker et al. (2018) write that these vulnerabilities ultimately could allow malicious actors to "violate the security assumptions underpinning numerous software security mechanisms" and "represent a serious threat to actual systems… that are used in billions of devices." The vulnerabilities could allow malicious actors to steal information stored in the processor memory, affecting virtually all computing devices, such as personal computers, cloud servers, and smartphones.

D. 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.

Cloud computing platforms are running using 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

[9] Project Zero. "Reading privileged memory with a side-channel." 01/03/2018. https://googleprojectzero.blogspot.com/2018/01/reading-privileged-memory-with-side.html.
[10] 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.

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).

4. 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 a security breach before a firm can. 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 the fear of negatively affecting its market value as well as 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 does the United States. 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. Cybersecurity professionals 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.

A. 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 $70 billion that Uber commanded just over a year ago (Reuters 2017b). While not all of the decline in value can be attributed to the data breach as Uber faced other negative publicity, offers following the breach 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).[11,12]

5. The cost of malicious cyber activity for the U.S. economy

The total cost of malicious cyber activity directed at U.S. entities is difficult to estimate because, as discussed above, many data breaches go undetected, and even when they are detected, they are mostly unreported, or the final cost is unknown. While no one has the complete data on adverse cyber events experienced by firms, cyber insurance firms are arguably in the best position to collect reliable data. Firms that sell cyber insurance products need to use probability assessments and expected cost estimates for adverse cyber events in order to price their products. Moreover, insurance firms are best able to collect unbiased datasets because they track the same firms over time and are able to observe otherwise undisclosed cyberattacks and data breaches. Unfortunately, insurance pricing data are considered proprietary and are not publicly available.

The losses suffered by the corporate sector as the result of malicious cyber activity extend beyond the direct losses suffered by firms that are attacked. These additional costs arise from

[11] Attorney General of the State of New York, Internet Bureau, Assurance No. 15-185.
[12] 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.

(1) spillover effects to economically linked firms, (2) increasing expenses on cybersecurity defense measures, and (3) a drag on economic growth that cyber threats create. We describe these costs in more detail below.

An attack may have significant spillover effects to corporate partners, customers, and suppliers. 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 news of the original compromise of Equifax's security.

Firms also incur non-negligible costs associated with preventing cyberattacks and data breaches and must acquire security products (e.g. spam filters, antivirus protection), offer services for consumers (training), and engage in other fraud detection and tracking efforts (Anderson et al. 2012). Cybersecurity expenditures, including antivirus technologies and other cleanup and defense expenditures, amounted to $24.8 billion globally in 2010-2012 (Anderson et al. 2012). PwC (2014) reports that an average firm spends about 4 percent of its information technology (IT) budget on cybersecurity, and more than 50 percent of firms have plans to increase their cybersecurity budgets by 5 percent or more in 2018, among which 42 percent of firms are expected to increase spending by at least 10 percent. 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 $128B market by 2020. The Equifax data breach resulted in significant share price increases for cybersecurity firms, indicating that the market revised up its expectations of the cybersecurity firms' future revenues.

We are reluctant to ascribe the cost of cyber protection as a deadweight cost to the U.S. economy, as employment in the cybersecurity sector contributes significantly to economic growth. Innovative technology solutions developed by the sector may generate positive spillover effects elsewhere in the economy. Finally, a sophisticated cybersecurity sector could become a reliable source of exports of both products and services for many years to come. To fill this future demand, the U.S. government may guide the development of the sector through educational programs that stimulate students' interest in cyber defense and should aid the recruitment of women, who are severely underrepresented in the field.

Finally, malicious cyber activity imposes a drag on economic growth by enabling new means for stealing IP, which can be considered a tax on innovation. The ever evolving cyber threats slow down the rate of development and adoption of new information and communications technologies and thereby lower the efficiency gains that can be achieved with these new technologies (see, e.g., Hughes, Bohl, Irfan, Margolese-Malin and Solorzano (2017)) for a detailed discussion and analysis of these and related effects).

When estimating total economic costs of malicious cyber activity against the U.S. economy, one should not overlook the substantial direct cost imposed on the government sector. Using

a dataset of cyber incidents from Advisen, a for-profit organization that collects and resells data from commercial insurance industry and public news sources, Romanosky (2016) estimates that the government sector is at highest risk for a cyber incident.[13]

According to the Government Accountability Office (2017), the number of cyber incidents reported by federal agencies rose substantially between FY2006 and FY2016 (from 5,503 to 33,632 incidents). However, FY2016 was a break from the consistent annual rise, as the number of reported incidents fell by 56 percent from the fiscal year prior. In a highly publicized incident, between 2014 and 2015, the Office of Personnel Management (OPM) suffered a security failure in which SF86 data were breached for 21.5 million individuals, including 5.6 million sets of fingerprints (OPM 2015). Another separate cyber incident involving personnel records occurred in 2015, which impacted 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 the box below illustrates a very costly cyber theft from the U.S. government (Capaccio 2017).

Case Study: Theft of U.S. Military Secrets through Cyber Means (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 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, as 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 FY2017 on development and production for the F-35 (DOD 2015c).

[13] Risk to a given sector is defined as the number of cyber incidents divided by the number of firms/agencies in a sector.

Evidence from state and local governments suggest cyber risks are pervasive there as well. Data breaches or compromises have the potential to affect thousands or even millions of individuals through the release of personal or sensitive information or disruption to government service provision. Responses to a 2013 survey of state and local government officials suggested that officials often underestimate the prevalence and potential severity of malicious cyber activity (Center for Digital Government 2014), and the Security Scorecard 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 particularly concerning rates of increase, 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).

Finally, malicious cyber activity imposes 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.

Using the information provided in this document, as well as estimates from Ponemon (2017) on the probability of a material data breach, we estimate that malicious cyber activity costs the U.S. economy between $57 billion and $109 billion in 2016, which represents between 0.31 percent and 0.58 percent of that year's GDP (please the Computational Appendix for the details). For comparison, based on an extrapolation exercise that used a variety of datasets on adverse cyber events from several countries, the Center for Strategic and International Studies (2014) estimates that the cost of malicious cyber activity directed at U.S. entities was $107 billion in 2013, which represented 0.64 percent of GDP.[14]

[14] For further comparison, the 2017 IP Commission Report estimates that the total cost to the U.S. economy stemming from IP theft perpetuated by any means by China and other infringers exceeds $255 billion a year.

The ongoing economic costs of malicious cyber activity estimated above likely amount to only a small fraction of the cost that the U.S. economy may incur if the United States were to enter a large-scale conflict in cyber space. We will discuss this scenario next.

6. Devastating cyberattack scenarios

Cybersecurity professionals, both in private and public sectors, stress that the potential costs of cyberattacks could far exceed the ongoing costs suffered by the U.S. economy. Following the worst terrorist attack in U.S. history, the 9/11 Commission concluded that the attacks revealed a failure in imagination. The commission stated that "it is therefore crucial to find a way of routinizing, even bureaucratizing, the exercise of imagination." Much effort is being expended by the cyber defense community to proactively anticipate the most devastating cyberattack vectors.

The cyber defense community is particularly concerned about attacks on so-called critical infrastructures, which are crucially important for a smooth functioning of the U.S. economy. Among the previously described 16 critical infrastructure sectors, we will focus in detail on the Financial Services Sector and the Energy Sector, more specifically, on the electric grid. These sectors are internally interconnected and interdependent with other sectors as well as robustly connected to the internet, and are thus at a highest risk for a devastating cyberattack that would ripple through the entire economy. Below, we focus on the current concerns and ongoing efforts to make these sectors more secure.

A. 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.

i. Malicious cyber activity directed at banks in the SWIFT network

The Society for Worldwide Interbank Financial Telecommunications (SWIFT) is a global member-owned cooperative and the world's leading provider of secure financial messaging services. Its messaging platform, products and services connect more than 11,000 banking and securities organizations in more than 200 countries and territories. SWIFT does not hold funds or manage accounts on behalf of customers; instead, it enables users to securely communicate standardized financial messages in order to set up subsequent account transfers.

In March 2016, the Bank of Bangladesh reported that over $81 million had been stolen from its account at the Federal Reserve Bank of New York. Hackers, who in the weeks prior had gained access to the Bank of Bangladesh's systems, had sent messages through the SWIFT system to the New York Fed, requesting the transfer of nearly one billion dollars in Bangladeshi reserves to accounts in the Philippines and Sri Lanka. Of these requests, the vast majority were not acted upon by the New York Fed due to formatting irregularities and the fortuitous usage of key words linked to Iranian sanctions. However, four of the 35 requests were acted upon and $81 million were transferred out of the Bank of Bangladesh's reserve accounts and subsequently laundered through the Filipino casino industry (Kittichaisaree 2017).

Since the disclosure of the theft from the Bank of Bangladesh, a number of similar thefts have come to light. It has since been revealed that in 2015 hackers used stolen SWIFT credentials to successfully transfer over $12 million from Wells Fargo accounts owned by Banco Del Austro (Banco Del Austro, S.A. v. Wells Fargo Bank, N.A., 2016) and that over $60 million was stolen from the Taiwanese Far Eastern International Bank. Analysis by cybersecurity firms, including Symantec, indicate that these cyber thefts are not isolated incidents. Evidence suggests that, since 2013, banks have been targeted by a group identified as Carbanak. Neither of the involved banks, nor SWIFT or the U.S. Government have made statements assigning blame. However numerous cybersecurity firms have conducted independent analyses and found links to other malicious cyber activity; they attributed these activities to the "Lazurus Group," a high level hacking group with purported links to North Korea. The group has been active since 2009 and is widely believed to be responsible for cyberattacks against other financial institutions and Sony Pictures.

In response to the escalating attacks, SWIFT launched a new Customer Security Intelligence Team as well as a 24/7 Security Operations Center to better monitor, detect, and react to security threats. Additionally, in March 2017, the New York Department of Financial Services implemented a new set of cybersecurity regulations emphasizing a more regulated approach to data privacy and disclosure as well as a more robust management of risk in an environment of escalating cybersecurity threats.

ii. Malicious cyber activity affecting financial markets

Malicious cyber activities directed at securities exchanges that compromise order execution and price efficiency have been reported in recent years. The International Organization of Securities Commissions (2013) reports, based on a survey of 46 global securities exchanges, that 53 percent had experienced malicious cyber activity. Fortunately, none reported losses as a result of these malicious activities amounting to greater than $1 million. The cyber events

were generally disruptive instead of being financially damaging. The most common forms of attack were DDoS and malware attacks (IOSCO 2013).[15]

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 have 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 malicious 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 and data breaches in 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 view 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.

[15] A malware attack is conducted through the use of harmful software.

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.

B. Power grid

An attack on the power grid could have devastating consequences for firms and private citizens.

i. Power grid attack vectors

Lloyd's 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. One such example is the December 2016 attack 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." The software, known as Crash Override, can only be detected if the system is actively sending out signals and can cut power for up to a few days in portions of a country. Crash Override is currently capable of attacking power operators across Europe but could be modified to work against the U.S. Crash Override is only the second malware engineered to disrupt industrial control processes (the first was Stuxnet in 2010) (Wired 2017).

According to the scenario, a particular threat actor (e.g., a nation-state) could develop a malware that can infect electricity generation control rooms. Methods for inserting the malware include, but are not limited to: (1) targeting laptops and other personal electronic devices of key personnel with access to multiple power plants, (2) conducting 'phishing' attacks that allow the hackers to compromise the corporate network and establish chain attacks that ultimately lead to the control system (known as pivoting), (3) hacking a remotely accessed control system, and (4) physically entering the locations that monitor the network.

Once the hackers succeed in inserting the malware into the control system, they could keep the malware dormant while it reports information and receives commands. Modern power

companies are vulnerable to such threats since they may mistake additional traffic on their systems as merely a fault or a vendor diagnostic connection.

The attackers can then choose to trigger the malware at their discretion and take control of the generators. They can accomplish this task by forcing the generators to overload and burn out, thus causing additional fires and explosions in some cases. Such an attack could potentially destabilize a large area, such as the entire Northeastern U.S. regional grid. Power could be restored in some areas relatively quickly (within 24 hours), but other areas may be left without power for a number of weeks (Lloyd's of London. 2015).

ii. Potential costs of attacks

A cyberattack on the electrical grid could have large-scale economic impacts as infrastructure damages, loss in output, delayed production, spoiled inventory, and loss of wages all decrease productivity and earnings for the duration of the blackout. Since there are no examples of successful past cyberattacks against the power grid in the U.S., potential damages have to be assessed from adverse weather conditions.

Another example is the August 14, 2003, power outage that affected the Midwest and Northeast United States, as well as parts of Canada, which was attributed to a programming error. The blackout was not weather-related; it lasted two days in most areas, and up to two weeks in some areas, making it the largest power outage in recent history with estimated cost of $6 billion (Minkel 2008).

According to the study conducted by Lloyd's and the University of Cambridge's Centre for Risk Studies, a large-scale cyberattack can lead to both direct and indirect damages. Direct damages would include, but are not limited to, damage to assets, infrastructure, sales revenue of electricity supply companies, sale revenue of other businesses and supply chains. The study estimates that such a malware attack would lead to a $243 billion to $1 trillion loss to the U.S. economy. Indirect costs would include consequences such as the loss to the insurance market. The study estimates that such an attack could cost the insurance industry $21.4 billion to $71.1 billion dollars. This figure could further increase when the calculation takes into account the wide range of claims that could be triggered.

The study also highlighted the specific impacts an attack of this type would have on the economy. Productivity would see a decrease as businesses close from loss of power and people are unable to perform their regular duties. Even as businesses return to power employees may have difficulties getting to work due to limited fuel supply, disabled traffic lights, and limited to no public transportation.

Trade will also be impacted as maritime operating ports are suspended and the ability to load and unload ships becomes difficult to impossible without electricity. In addition, even if goods are able to make it to the limited available ports, there would be backups resulting in a slowdown of production along the supply chain.

Consumption will increase initially as people panic buy commodities; however, this will quickly take a turn. As banks do not have power and businesses either have to close or are limited to cash, people will need to limit their consumption and it will remain low until all affected people and business return to full power.

Finally, rail systems and airports will be shut down as a result of the power outages impacting tourism. The study expects that tourism would decrease severely during the outage and would not return to normal levels for several weeks.[16]

iii. Health and safety

In addition to the economic impacts of a large power outage, there are health and safety concerns. Power outages impacting heating and cooling systems, at home health systems, refrigeration, and slower emergency response will all increase the rate of illnesses and death in the impacted areas. People will suffer from heat related conditions (such as heat stroke) and hypothermia, spoiled food, and difficulty of emergency responders to communicate with those impacted. In addition, riots, looting, and arson attacks as well as lack of lighting and overstretched police will increase crimes and decrease safety.

Water and sewage facilities will also be impacted. There will be a limited supply of clean water as the power outage will impact pumps. This will result in people either having to go without water, using a limited portable water supply, and/or drinking contaminated water. Sewage plants will also experience spills as the facilities will not be able to operate without power (Lloyd's of London 2015).

Finally, hospitals will see a shortage of fuel for backup generators. With the average generator able to hold fuel to provide eight hours of power, a run on the fuel supply as well as high demand will limit the amount that can get to hospitals and other high need locations.

iv. National security

Currently, 85 percent of the DoD's energy comes from commercial sources. The Department "recognizes that such events could result in power outages affecting critical DoD missions

[16] Please see the footnote above.

involving power projection, defense of the homeland, or operations conducted at installations in the U.S."

It is estimated that a loss of power would impact the DoD missions of preventing terrorism and enhancing security, safeguarding and securing cyberspace, and strengthening national preparedness. If power outages affected missions both at home and abroad, United States security would be significantly impacted.[17]

v. Trust

FireEye Horizons published a report in which they noted that an attack could hinder the trust between a government and the people, citing the example of Russian interference in the U.S. Election and the questions surrounding the allegations and the security of the election process. The study explains that, even though no infrastructure was harmed, the "trust placed in the process has been degraded".[18]

An attack on the United States electrical grid could impact consumers' trust in their electrical company and the government security. While this would likely not prevent people from purchasing electricity, it could raise questions regarding national security and consumer safety.

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 using various attack vectors as well as various methods of defense in order to determine the most effective form of defense against the possible attack scenarios.

Cybersecurity experts like to say that in a future war the first shots will be fired in cyberspace. A growing consensus indicates that cyberspace is already being used by nation-states for retaliation against sanctions imposed on them by the international community.

A cyber adversary can utilize numerous attack vectors simultaneously. The back doors that were previously established may be used to concurrently attack the compromised firms for the purpose of simultaneous business-destruction type of attacks that was previously observed in case of Sony. An attack launched against the electric grid could affect large swaths of the U.S. economy because most economic activity is dependent on access to electricity. Financial markets could be attacked as well to reduce trust in the financial system. Economic analysis conducted by various industry studies estimates that cyberattacks on critical infrastructure assets can cause damage up to $1 trillion (Tofan 2016; Lloyd's of London 2015, 2017).

[17] Section 2(e): Assessment of Electricity Disruption Incident Response Capabilities

[18] FireEye Horizons: Smart Cities Growth Presents Opportunities for State Coercion, August 2016.

7. Initiatives to reduce cyber risk

Defending against cyber threats requires building effective and evolving cyber capabilities that span all entities in the U.S. economy. Multiple efforts across the public and private sectors are already underway to address cyber concerns.

A. Public sector initiatives

Government involvement in improving cybersecurity can take many forms. A number of regulations push firms to internalize the externalities associated with lax cybersecurity, for example, by mandating disclosure and by penalizing firms for certain data breaches, as exemplified by the SEC 2011 Cybersecurity Disclosure Guidance, DOE's Electric Emergency Incident and Disturbance Report (DOE 2017), and the EU's General Data Protection Regulation (GDPR 2017). The government can also facilitate information sharing, such as through the Department of Homeland Security's Automated Indicator Sharing (AIS) Program (DHS 2016).

Government investment in basic research on cyber protection leverages economies of scale. For example, in FY2018, DARPA allocated about 10 percent ($41.2 million) of its research budget to cyber sciences (DARPA 2017). The investment in basic research historically spurred further innovation by the private sector. For example, DARPA's basic research investments in Unmanned Aerial Vehicle (UAVs) have spurred innovation in the private aerospace industry (DARPA 2015).

Standard-setting is another path to ensure that companies are aware of best cybersecurity practices. The NIST Cybersecurity Framework, which recognizes five critical functions for managing cybersecurity risk: to identify, protect, detect, respond, and recover from cyber risks, creates a common lexicon for cybersecurity issues. It is an example of a standards tool that was originally targeted for critical infrastructure but then adopted by the broader government community (including other counties, such as Italy) and increasingly by the private sector (NIST 2017).

Effective law enforcement, a function performed by government, is critical for discouraging malicious cyber activity, 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 malicious cyber activity. 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, including many that were located abroad. As an example of a successful operation, in April 2017, DOJ played an active role in disrupting the Kelihos botnet (DOJ 2017a).

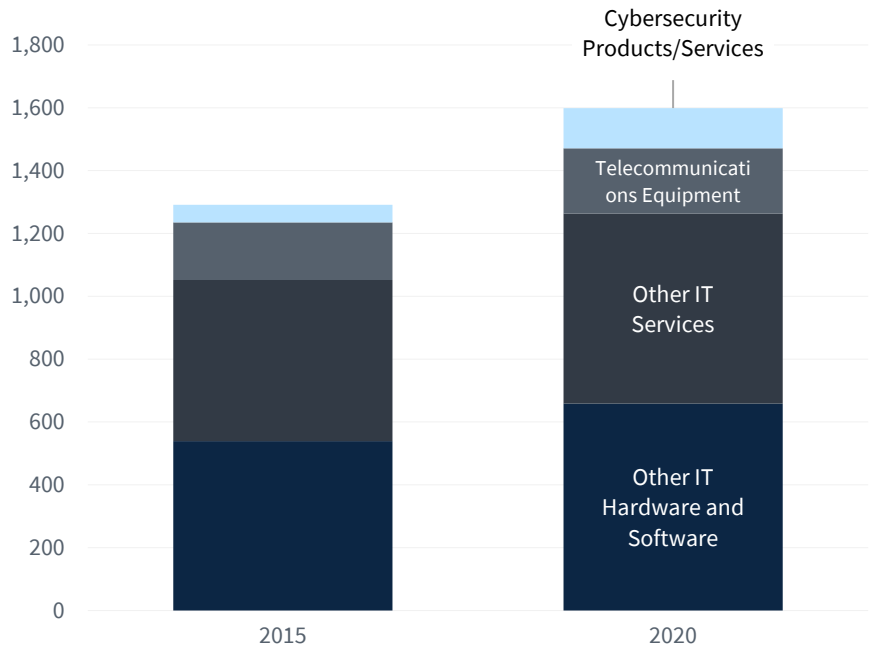
The government can also engage in building international consensus on cyber protection and creating a strong pipeline into the cybersecurity workforce through various efforts, such as by promoting early exposure to STEM education and engaging in international forums—such as the G-7, G-20, and Financial Stability Board, on cybersecurity issues in the financial sector. The government is also involved in educating consumers and spurring demand for secure products. For example, the Department of Homeland Security's Stop.Think.Connect Campaign is designed to increase public awareness of cyber threats. Finally, the government plays an active role in protecting critical infrastructure assets: Executive Order 13800 on "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" includes efforts to improve cybersecurity risk management across critical infrastructures.

B. Private sector initiatives

While government can help address some elements of cyber protection issues, the most direct actions in cybersecurity are in the hands of the private sector. Private firms are ultimately in the best position to figure out the most appropriate sector- and firm-specific cybersecurity practices.

Figure 9. Investment Projections in Cybersecurity

(Billions of Dollars)



Source: Morgan and Stanley (2016).

Morgan Stanley (2016) estimates that spending on cybersecurity products and services will 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 9). Cybersecurity spending may be used for a variety of technologies, such as security intelligence systems (which Ponemon 2017a notes as the most frequently used in its sample of firms), blockchain technology, designed to preserve record integrity, and sophisticated authentication procedures to better protect data and networks.

Additionally, the private sector strives to improve inter-firm information sharing. For example, industry-led Information Sharing and Analysis Centers (ISACs) have formed across sectors, which "collect, analyze, and disseminate actionable threat information" to members on cyber threats (National Council of ISAC 2017). Information Sharing and Analysis Organizations (ISAOs), facilitated by the Department of Homeland Security, meanwhile, seek to create "transparent best practices" addressing the needs of all industry groups through an "open-ended public engagement" led by the Standards Organization (DHS 2016). Other developments in the private sector include a quick growth of the cyber insurance market, which helps firms share the risks of adverse cyber events, and the emergence of the cybersecurity sector, which manages cyber protection for an increasing number of corporate customers.

Conclusion

Cyber connectivity is an important driver of productivity, innovation, and growth for the U.S. economy, but it comes at a cost. Companies, individuals, and the government are vulnerable to malicious cyber activity. Effective public and private-sector efforts to combat this malicious activity would contribute to domestic GDP growth. However, the ever-evolving nature and scope of cyber threats suggest that additional and continued efforts are critical, and the cooperation between public and private sectors is key.

References

Accenture. 2016. “Chief Supply Chain Officers.” https://www.accenture.com/t20161216T015905Z__w__/us-en/_acnmedia/PDF-25/Accenture-Strategy-Supply-Chain-Cybersecurity-POV.pdf.

American Bar Association. 2016. “Vendor Contracting Project: Cybersecurity Checklist.” https://www.americanbar.org/content/dam/aba/images/law_national_security/Cybersecurity%20Task%20Force%20Vendor%20Contracting%20Checklist%20v%201%2010-17-2016%20cmb%20edits%20clean.pdf.

Anderson, Ross, Chris Barton, Rainer Böhme, Richard Clayton, Michel J. G. van Eeten, Michael Levi, Tyler Moore, and Stefan Savage. 2012. Measuring the Cost of Cybercrime. 11th Workshop on the Economics of Information Security, Berlin Germany. http://www.econinfosec.org/archive/weis2012/presentation/Moore_presentation_WEIS2012.pdf.

Banco Del Austro, S.A., v. Wells Fargo Bank, N.A., (No. 16-cv-00628). Retrieved from https://law.justia.com/cases/federal/district-courts/new-york/nysdce/1:2016cv00628/452772/27/.

Barry B. Hughes, David Bohl, Mohammod Irfan, Eli Margolese-Malin, José R. Solórzano. 2017. “ICT/Cyber benefits and costs: Reconciling competing perspectives on the current and future balance, Technological Forecasting and Social Change”, Vol. 115, 117-130. https://www.sciencedirect.com/science/article/pii/S0040162516303560.

Bossert, T. 2017. “It’s Official: North Korea Is Behind WannaCry.” Op-ed, Wall Street Journal, December 18.

Capaccio, A. 2017. “F-35 Program Costs Jump to $406.5 Billion in Latest Estimate.” Bloomberg News, July 10. https://www.bloomberg.com/news/articles/2017-07-10/f-35-program-costs-jump-to-406-billion-in-new-pentagon-estimate.

Center for Digital Government. 2014. Advanced Cyber Threats in State and Local Government. http://www.nascio.org/events/sponsors/vrc/Advanced%20Cyber%20Threats%20in%20State%20and%20%20Local%20Government.pdf.

Chang, J. 2014. The Dark Cloud of Convenience: How the HIPAA Omnibus Rules Fail to Protect Electronic Personal Health Information. Loyola of Los Angeles Entertainment Law Review, 34(2), 119-154.

Cichonski, P., T. Millar, T. Grance, and K. Scarfone. 2012. Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology.

Special Publication 800-61. https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final.

CSIS (Center for Strategic and International Studies). 2014. "Net Losses: Estimating the Global Cost of Cybercrime," June.

CUNA (Credit Union National Association). 2014. "Home Depot Breach Cost CUs Nearly Double Those from Target." October 30. http://news.cuna.org/articles/Home_Depot_breach_cost_CUs_nearly_double_those_from_Target.

Customs Border Protection. FY2016 IPR Annual Seizure Statistics. https://2013portal.whca.mil/sites/CEA45/Shared%20Documents/Memos%20for%20other%20agencies/IP/IP%20Theft%20Cost/IP%20Theft%20LB%20UB%20v2.xls?Web=1.

DARPA (Defense Advanced Research Projects Agency). 2015. Breakthrough Technologies for National Security. https://www.darpa.mil/attachments/DARPA2015.pdf.

DARPA (Defense Advanced Research Projects Agency). 2017. Department of Defense FY 2018 Budget Estimates. https://www.darpa.mil/attachments/DARPA_FY18_Presidents_Budget_Request.pdf.

DHS (Department of Homeland Security). 2016. Automated Indicator Sharing (AIS) Program. https://www.dhs.gov/ais.

DHS (Department of Homeland Security). 2017b. "Critical Infrastructure Sectors." https://www.dhs.gov/critical-infrastructure-sectors.

DHS (Department of Homeland Security). 2017d. "National Cybersecurity Workforce Framework." https://niccs.us-cert.gov/.

Digital Attack Map. 2017. "Top Daily DDoS Attacks Worldwide." http://www.digitalattackmap.com/understanding-ddos/.

DiMasi, Joseph A., and Henry G. Grabowski. 2007. "Economics of New Oncology Drug Development." Journal of Clinical Oncology. Vol. 25 (2), 209-216.

DNI (Director of National Intelligence). 2017. World Threat Assessment of the U.S. Intelligence Community.https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Unclassified%20SFR%20-%20Final.pdf.

DOD (Department of Defense). 2015a. The Department of Defense Cyber Strategy. https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

DOD (Department of Defense). 2015. What is Security Analysis? DOD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework into the System Acquisition Lifecycle. https://www.dau.mil/tools/Lists/DAUTools/Attachments/37/DoD%20-%20Guidebook,%20Cybersecurity%20Risk%20Management%20Framework,%20v1.08,%20Sep%202015.pdf.

DOE (Department of Energy). 2017. Electric Disturbance Events (OE-47) Annual Summaries. https://www.oe.netl.doe.gov/OE417_annual_summary.aspx.

DOJ (Department of Justice). 2014. "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage." https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

———. 2016a. "Computer Hacking Conspiracy Charges Unsealed Against Members of Syrian Electronic Army." https://www.justice.gov/opa/pr/computer-hacking-conspiracy-charges-unsealed-against-members-syrian-electronic-army.

———. 2016c. "Chinese National Pleads Guilty to Conspiring to Hack into U.S. Defense Contractors' Systems to Steal Sensitive Military Information."

———. 2017a. "Justice Department Announces Actions to Dismantle Kelihos Botnet." https://www.justice.gov/opa/pr/justice-department-announces-actions-dismantle-kelihos-botnet-0.

Domm, P. 2013. "False Rumor of Explosion at White House Causes Stocks to Briefly Plunge; AP Confirms Its Twitter Feed Was Hacked." Market Insider, CNBC, April 23. https://www.cnbc.com/id/100646197.

Dyn. 2016. "Dyn Statement on 10/21/2016 DDoS Attack." October 22. https://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/.

EAC (U.S. Election Assistance Commission). 2017. "Starting Point. U.S. Election Systems as Critical Infrastructure." https://www.eac.gov/assets/1/6/starting_point_us_election_systems_as_Critical_Infrastructure.pdf.

E-ISAC (Electricity Information Sharing and Analysis Center). 2016. E-ISAC End of Year Report. file:///C:/Users/langburd_n2/Work%20Folders/Downloads/E-ISAC%202016%20End%20of%20Year%20Report.pdf.

Elkind, P. 2015. "The Cyber Bomb is Detonated." http://fortune.com/sony-hack-final-part/.

Equifax. 2017a. "Equifax Announces Cybersecurity Incident Involving Consumer Information." September 7. https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628.

Equifax. 2017b. "Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes." September 15. https://investor.equifax.com/news-and-events/news/2017/09-15-2017-224018832.

Equifax. 2017c. "Equifax Board Releases Findings of Special Committee Regarding Stock Sale by Executives." November 3. https://investor.equifax.com/news-and-events/news/2017/11-03-2017-124511096.

FBI (Federal Bureau of Investigation). 2014. "Update on Sony Investigation." https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation.

FBI (Federal Bureau of Investigation). 2017. Intellectual Property Theft/Piracy. https://www.fbi.gov/investigate/white-collar-crime/piracy-ip-theft.

Ferraro, M. F. 2014. "Groundbreaking' or Broken? An Analysis of SEC Cybersecurity Disclosure Guidance, Its Effectiveness, and Implications," Albany Law Review, Vol. 77, 297-347.

Fialka, John. 2016. "Why China Is Dominating the Solar Industry." https://www.scientificamerican.com/article/why-china-is-dominating-the-solar-industry/.

Finkle, J. "Exclusive: FBI warns of 'destructive' malware in wake of Sony attack." https://www.reuters.com/article/us-sony-cybersecurity-malware/exclusive-fbi-warns-of-destructive-malware-in-wake-of-sony-attack-idUSKCN0JF3FE20141202.

FireEye. 2016. "Redline Drawn: China Recalculates Its Use of Cyber Espionage." https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf.

Frontier Economics. 2011. "Estimating the Global Economic and Social Impacts of Counterfeiting and Piracy."

GAO (Government Accountability Office). 2017. "Cybersecurity Actions Needed to Strengthen U.S. Capabilities." https://www.gao.gov/assets/690/682756.pdf.

GDPR (EU General Data Protection Regulation). 2017. GDPR Portal. https://www.eugdpr.org/.

Geers, Kenneth. 2014. "Pandemonium: Nation States, National Security, and the Internet." The NATO Cooperative Cyber Defence Centre of Excellence. https://www.ccdcoe.org/publications/TP_Vol1No1_Geers.pdf.

Gordon, L., M. Loeb, W. Lucyshyn, and T. Sohail. 2006. "The Impact of the Sarbanes-Oxley Act on the Corporate Disclosures of Information Security Activities." Journal of Accounting and Public Policy 25: 503–30.

Gordon, Lawrence A., Martin P. Loeb, William Lucyshyn, and Lei Zhou. 2015. "Externalities and the Magnitude of Cybersecurity Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model," Journal of Informational Security, Vol. 6, 24-30.

Gregory, H. J. 2014. "SEC Review of Disclosure Effectiveness," Practical Law Journal, June 28-31.

Guo, Jeff. 2014. "The Postal Service is losing millions a year to help you buy cheap stuff from China." Washington Post, September 12. https://www.washingtonpost.com/news/storyline/wp/2014/09/12/the-postal-service-is-losing-millions-a-year-to-help-you-buy-cheap-stuff-from-china/?utm_term=.6311c58a7d73.

Hilary, Gilles, Benjamin Segal and May H. Zhang. 2016. "Cyber-Risk Disclosure: Who Cares?" Georgetown University McDonough School of Business Working Paper.

Hiscox. 2017. "Hiscox Cyber Readiness Report 2017." http://www.hiscox.com/cyber-readiness-report/.

The Home Depot, Inc. 2014a. "The Home Depot Completes Malware Elimination and Enhanced Encryption of Payment Data in All U.S. Stores." http://ir.homedepot.com/news-releases/2014/09-18-2014-014517752.

———. 2014b. "The Home Depot Reports Findings in Payment Data Breach Investigation." http://ir.homedepot.com/news-releases/2014/11-06-2014-014517315.

———.2017. "2016 Annual Report." http://ir.homedepot.com/~/media/Files/H/HomeDepot-IR/reports-and-presentations/annual-reports/annual-report-2016.pdf.

Hughes, B., D. Bohl, M. Irfan, E. Margolese-Malin, and J. Solórzano. 2017. "ICT/Cyber Benefits and Costs: Reconciling Competing Perspectives on the Current and Future Balance." Technological Forecasting and Social Change 115: 117–30. https://www.sciencedirect.com/science/article/pii/S0040162516303560.

Ignatius, A. 2015. "'They Burned the House Down': An Interview with Michael Lynton." https://hbr.org/2015/07/they-burned-the-house-down.

IOSCO (International Organization of Securities Commissions) and the World Federation of Exchange Office, 2013, "Cybercrime, Securities Markets and Systemic Risk," July.

IP Commission. 2017. “Update to the Report of the Commission on the Theft of American Intellectual Property.” http://www.ipcommission.org/report/ip_commission_report_052213.pdf.

Isaac, M., K. Benner, and S. Frenkel. 2017. “Uber Hid 2016 Breach, Paying Hackers to Delete Stolen Data.” New York Times, November 21. https://www.nytimes.com/2017/11/21/technology/uber-hack.html.

Jin, Jingjing. 2015. “Cybersecurity Disclosure Effectiveness on Public Companies,” James Madison University senior honors thesis.

Kittichaisaree, Kriangsak. Public International Law of Cyberspace. Switzerland: Springer International Publishing, 2017. Print.

Koch, D. D. 2016. Is the HIPAA Security Rule Enough to Protect Electronic Personal Health Information (PHI) in the Cyber Age? Journal of Health Care Finance, Vol. 43 (3), 1-32.

Koch, D. 2017. “Is the HIPAA Security Rule Enough to Protect Electronic Personal Health Information (PHI) in the Cyber Age?” Journal of Health Care Finance 43, no. 3: 1–32.

Kocialkowski, Paul. 2014. “Replicant developers find and close Samsung Galaxy backdoor,” Free Software Foundation. March 12.

Kocialkowski, Paul. 2014. “Samsung Galaxy back-door.” Replicant Forums. March 2, https://redmine.replicant.us/projects/replicant/wiki/SamsungGalaxyBackdoor.

Kocker P, Genking D, Gruss D, Haas W, Hamburg M, Lipp M, Mangard S, Prescher T, Schwarz M, Yarom Y. 2018. “Specter Attacks: Exploiting Speculative Execution,” University of Pennsylvania and Maryland. https://spectreattack.com/spectre.pdf.

Krebs on Security. 2016. “Hacked Cameras, DVRs Powered Today’s Massive Internet Outage.” October. https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/.

Kvochko, Elena and Rajiv Pant. 2015. “Why Data Breaches Don’t Hurt Stock Prices.” Harvard Business Review, March 31.

Lee, Hau. L. and Pamela Passman. 2014. “How Companies Can Protect Themselves Against Intellectual Property Risk in Their Supply Chains.” https://www.gsb.stanford.edu/insights/how-companies-can-protect-themselves-against-intellectual-property-risk-their-supply-chains.

Lloyd’s of London. 2015. Business Blackout: The Insurance Implications of a Cyberattack on the U.S. Power Grid. University of Cambridge Centre for Risk Studies.

https://www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/business%20blackout/business%20blackout20150708.pdf.

Lloyd's of London. 2017. Counting the cost - Cyber exposure decoded. July 17. https://www.lloyds.com/news-and-insight/risk-insight/library/technology/countingthecost.

Newcomer, E. 2017. "Uber Paid Hackers to Delete Stolen Data on 57 Million People." Bloomberg. https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data.

McAfee and CSIS. 2014. Stopping Cybercrime Can Positively Impact World Economies. https://www.mcafee.com/us/about/news/2014/q2/20140609-01.aspx.

McAfee Labs. November 2016. "2017 Threat Predictions." https://www.mcafee.com/us/resources/reports/rp-threats-predictions-2017.pdf.

———. 2017. "McAfee Labs 2017 Threat Predictions Report." https://www.mcafee.com/us/resources/reports/rp-threats-predictions-2017.pdf.

Minkel, JR. 2008. "The 2003 Northeast Blackout---Five Years Later." Scientific American. https://www.scientificamerican.com/article/2003-blackout-five-years-later/.

MIT. 2015. "MIT Experts United to Combat Cybercrime," Spectrum. https://spectrum.mit.edu/continuum/mit-experts-unite-to-combat-cybercrime/.

Mitchell, M, and E. Stafford. 2000. "Managerial Decisions and Long-Term Stock Price Performance." Journal of Business 73, no. 3, 282–329.

Morgan Stanley. 2016. "Cybersecurity: Time for a Paradigm Shift," Morgan Stanley Research Paper, June 15.

Morgan Stanley. 2016. "Cybersecurity: Time for a Paradigm Shift." http://www.morganstanley.com/ideas/cybersecurity-needs-new-paradigm.

Nasdaq. 2017. "Equifax Panel Clears Executives Of Insider Trading But DOJ Probe Looms." November 3. http://www.nasdaq.com/article/equifax-panel-clears-executives-of-insider-trading-but-doj-probe-looms-cm871306.

National Association of ISACs. Accessed 7 November 2017.

National Conference of State Legislatures. 2017. "Security Breach Notification Laws." April 12, 2017.

National Council of ISACs. 2017. "About ISACs." https://www.nationalisacs.org.

National Cybersecurity Alliance. 2012. “America’s Small Businesses Must Take Online Security More Seriously,” October.

National Small Business Association. 2015. Year-End Economic Report. http://www.nsba.biz/wp-content/uploads/2016/02/Year-End-Economic-Report-2015.pdf.

Neuhierl, Andreas, Anna Scherbina and Bernd Schlusche. 2013. “Market Reaction to Corporate Press Releases,” Journal of Financial and Quantitative Analysis, Vol. 48 (4), 1207-1240.

New York State Office of the Attorney General. 2016. “A.G. Schneiderman Announces Settlement with Uber to Enhance Rider Privacy.” https://ag.ny.gov/press-release/ag-schneiderman-announces-settlement-uber-enhance-rider-privacy.

NIST (National Institute of Standards and Technology). 2012. Computer Security Incident Handling Guide. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

NIST (National Institute of Standards and Technology). 2016. “Dramatically Reducing Software Vulnerabilities.” https://doi.org/10.6028/NIST.IR.8151.

NIST (National Institute of Standards and Technology). 2017. Cybersecurity Framework. https://www.nist.gov/cyberframework.

Noveta Solutions. “Novetta Exposes Depth of Sony Pictures Attack.” https://www.novetta.com/2016/02/novetta-exposes-depth-of-sony-pictures-attack/.

OECD (Organization for Economic Cooperation and Development). 2008. “The Economic Impact of Counterfeiting and Piracy.” https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/resources/research-and-studies/Econ-Impacts-OECD_en.pdf.

OECD (Organization for Economic Cooperation and Development). 2016. "Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact." http://www.oecd.org/governance/trade-in-counterfeit-and-pirated-goods-9789264252653-en.htm.

OPM (Office of Personnel Management). 2015. “Statement by OPM Press Secretary Sam Schumach on Background Investigations Incident.” https://www.opm.gov/news/releases/2015/09/cyber-statement-923/.

OPM (Office of Personnel Management). 2017. Cybersecurity Resource Center. https://www.opm.gov/cybersecurity/.

OWASP (Open Web Application Security Project). 2006. OWASP 10 Most Common Backdoors. https://www.owasp.org/index.php/File:OWASP_10_Most_Common_Backdoors.pdf.

OWASP (Open Web Application Security Project). 2014. CISO Survey and Report 2013. https://www.owasp.org/images/2/28/Owasp-ciso-report-2013-1.0.pdf.

Patterson Belknap. 2017. "Home Depot Settles with Financial Institutions for Over 25 Million in Data Breach Case." https://www.pbwt.com/data-security-law-blog/home-depot-settles-with-financial-institutions-for-over-25-million-in-data-breach-case.

Ponemon Institute. 2014. Cost of Data Breach Study: Global Analysis. https://www-935.ibm.com/services/multimedia/SEL03027USEN_Poneman_2014_Cost_of_Data_Breach_Study.pdf.

Ponemon Institute. 2016. 2016 Cost of Cybercrime Study and the Risk of Business Innovation. https://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf.

Ponemon Institute. 2017a. Cost of Cybercrime Study.

Ponemon Institute. 2017b. Global Cyber Risk Transfer Comparison Report.

PwC (PricewaterhouseCoopers). 2014. "Managing Cyber Risks in an Interconnected World," September.

PwC (PricewaterhouseCoopers). 2017. "Operation Cloud Hopper." April.

Rai, Arti, Stuart Graham, and Mark Doms. 2010. Patent Reform: Unleashing Innovation, Promoting Economic Growth, and Producing High-Paying Jobs. White Paper. Department of Commerce. http://2010-2014.commerce.gov/sites/default/files/documents/migrated/Patent_Reform-paper.pdf.

Reuters. 2017a. "Security Firms Warn of New Cyber Threat to Electric Grid." https://www.reuters.com/article/cyber-attack-utilities/security-firms-warn-of-new-cyber-threat-to-electric-grid-idUSL1N1J61JK.

———. 2017b. "Softbank Succeeds in Tender Offer for Uber Shares." December 28. https://www.reuters.com/article/us-uber-softbank-tender/softbank-succeeds-in-tender-offer-for-uber-shares-idUSKBN1EM1NB.

Richwine, L. and J. Finkle. 2014. "Group claiming Sony hack demands 'Interview' not be released." https://www.reuters.com/article/us-sony-cybersecurity-hackers/group-claiming-sony-hack-demands-interview-not-be-released-idUSKBN0JM2IS20141209.

Rigby, Bill and Paul Carsten. 2015. "Microsoft Tackles China Piracy with Free Upgrade to Windows 10." Reuters. http://www.reuters.com/article/microsoft-china/microsoft-tackles-china-piracy-with-free-upgrade-to-windows-10-idUSL2N0WJ2N220150318.

Romanosky, Sasha. 2016. "Examining the Costs and Causes of Cyber Incidents," Journal of Cybersecurity, Vol 0, Issue 0.

Scherbina, Anna. 2008. "Suppressed negative information and future underperformance," Review of Finance, Vol. 12 (3), 533-565.

Scherbina, Anna and Bernd Schlusche. 2015. "Economic Linkages Inferred from News Stories and the Predictability of Stock Returns," Working paper, SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2363436.

Scherbina, Anna and Bernd Schlusche. 2016. "Cross-Firm Information Flows and the Predictability of Stock Returns," Working paper, SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2263033.

Scott, J., and D. Spaniel. 2016. "Rise of the Machines." http://icitech.org/wp-content/uploads/2016/12/ICIT-Brief-Rise-of-the-Machines.pdf.

SEC (Securities and Exchange Commission). 2011. CF Disclosure Guidance: Topic No. 2. Cybersecurity. https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

Security Scorecard. 2017. "2017 U.S. State and Federal Government Cybersecurity Research Report." https://explore.securityscorecard.com/us-government-cybersecurity-report.html.

Sony Corporation. 2014. "United States Securities and Exchange Commission Form 20-F." https://www.sony.net/SonyInfo/IR/library/FY2013_20F_PDF.pdf.

Sony Corporation. 2015. "Consolidated Financial Results for the Fiscal Year Ended March 31, 2015." https://www.sony.net/SonyInfo/IR/library/fr/14q4_sony.pdf.

Target Corporation. 2014. "Financial News Release." April 29. http://investors.target.com/phoenix.zhtml?c=65828&p=irol-newsArticle&ID=1923423.

Tofan, D. 2016. The cost of incidents affecting CIIs. European Union Agency for Network and Information Security. https://www.enisa.europa.eu/publications/the-cost-of-incidents-affecting-ciis/at_download/fullReport.

TruSight. 2017. "American Express, Bank of America, JPMorgan Chase and Wells Fargo Form Industry Consortium to Transform Third-Party Risk Management." https://trusightsolutions.com/sites/all/themes/nxtpm/assets/TruSight_Launch_Press_Release.pdf.

U.S. Commerce Department Patent and Trademark Office. 2016. "Intellectual Property and the U.S. Economy: 2016 Update." https://www.uspto.gov/sites/default/files/documents/IPandtheUSEconomySept2016.pdf.

U.S. Department of Justice. 2005. National Computer Security Survey 2005. https://www.bjs.gov/index.cfm?ty=tp&tid=41.

U.S. District Court Western District of Pennsylvania. 2014. Criminal Number 14-118: USA vs. Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, and Gu Chunui. https://www.justice.gov/iso/opa/resources/512201451913235846194 9.pdf.

USITC (United States International Trade Commission). 2011. China: Effects of Intellectual Property Infringement and Indigenous Innovation Politics on the U.S. Economy. https://www.usitc.gov/publications/332/pub4226.pdf.

USTR (United States Trade Representative). 2017a. 2017 Special 301 Report. https://ustr.gov/sites/default/files/301/2017%20Special%20301%20Report%20FINAL.PDF.

USTR (United States Trade Representative). 2017b. "Section 301 Hearing Transcript 10/10/2017." https://www.regulations.gov/document?D=USTR-2017-0016-0063.

USTR (United States Trade Representative). 2017c. "Initiation of Section 301 Investigation; Hearing; and Request for Public Comments: China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation." https://www.federalregister.gov/documents/2017/08/24/2017-17931/initiation-of-section-301-investigation-hearing-and-request-for-public-comments-chinas-acts-policies.

Verizon. 2013. 2013 Data Breach Investigations Report. http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf.

Verizon. 2015. 2015 Data Breach Investigations Report.

Verizon. 2017. 2017 Data Breach Investigations Report.

Wall Street Journal. 2014. "China's Cyber-Theft Jet Fighter; The New Stealth J-31 Is Modeled on the U.S. F-35." https://search.proquest.com/docview/1622947713/3FBEE0B0F08B4601PQ/1?accountid=45205.

Weisgerber, M. 2015. "China's Copycat Jet Raises Questions About F-35." http://www.defenseone.com/threats/2015/09/more-questions-f-35-after-new-specs-chinas-copycat/121859/.

Wired. 2015. "SEC Report Shows the Supply Chain Is More Like an Attack Chain." http://insights.wired.com/profiles/blogs/new-sec-report-shows-supply-chain-is-more-like-attack-chain#axzz4x6ZXsfBF.

Wired. 2017. "'Crash Override': The Malware that Took Down the Power Grid," June 12.

The 9/11 Commission Report, 2004.

The White House. 2013. "Presidential Policy Directive—Critical Infrastructure Security and Resilience." https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

The White House. 2017. "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal.

The (WTO) World Trade Organization. Dispute Settlement Cases. https://www.wto.org/english/tratop_e/dispu_e/find_dispu_cases_e.htm.

Wouk, Kris. 2015. "Update: Pirates Get Free Copies of Windows 10—But It Won't Be Genuine," Digital Trends. https://www.digitaltrends.com/computing/microsoft-free-windows-10-china/.

Wysopal, Chris and Eng, Chris. 2007. "Static Detection of Application Backdoors," Veracode, Incorporated.

Computational appendix

Ponemon (2017) uses survey results to estimate that an average probability that an organization experiences a material data breach in the next 24 months is 27.7 percent (page 1 of the document). This makes the annual probability of a material data breach 13.85 percent. According to our estimate in Table 1, an adverse cyber event cost firms 1.01% of their market value during the 2014 – January 2017 period. Since the dollar value of all publicly traded firms was $26.6 trillion in the fourth quarter of 2017[19], we estimate the total direct cost of malicious cyber activity directed at publicly traded firms to be 13.85%*1.01% *$26.6 trillion = $37.2 billion. We also estimate that the magnitude of spillover effects to economically linked firms was $9.2 billion.[20] Adding these costs together, we calculate that the total cost of malicious cyber activity directed at publicly traded firms was $46.5 billion, which amounted to 0.17% of the market value of all publicly traded firms. Applying this percentage cost to the value of all closely held firms and of the government sector, as per Table L.223, we estimate the costs of malicious cyber activity incurred by these sectors to be $8.7 billion and $0.4 billion, respectively. Finally, when estimating the cost incurred by private individuals, we adjust the total reported cost of $220 million, mentioned in this paper, for underreporting, and get the total cost estimate of $1.5 billion. Thus, the total estimate of the cost of malicious cyber activity to the U.S. economy equaled $57.1 billion in 2016, which represents 0.31% of that year's GDP.[21]

Our estimate represents the lower bound of the possible cost of malicious cyber activity because it accounts only for the cost of data breaches and does not attempt to quantify the dollar cost of other types of malicious cyber activity, such as DDoS attacks, ransom attacks, and destructive malware attacks. We therefore re-estimate the total cost of malicious cyber activity using a slightly different set of assumptions on the probability that a given firm experiences an adverse cyber event in a particular year.

We estimate the probability that a firm experiences any type of adverse cyber event by taking into account underreporting. To estimate the likelihood of underreporting, we refer back to the finding described earlier in the document that only one out of the 34 firms that was hacked at the same time as Google reported the crime publicly. These numbers suggest that the odds

[19] See Table L.223 of Financial Accounts of the United States produced by the Federal Reserve Board, https://www.federalreserve.gov/releases/z1/current/z1.pdf.

[20] To get to this number, we perform the following calculation. Scherbina and Schlusche (2015) report that a firm has significant economic linkages to 0.8 other firms, on average. Moreover, Scherbina and Schlusche (2016) estimate that a 1% return shock to a given firm causes a 0.32% return shock for economically linked firms. Hence, the dollar value of spillover effects will be roughly equal to 0.8*0.32*$37.2 billion.

[21] If spillover effects are not taken into account, we obtain a somewhat lower estimate of the total cost of malicious cyber activity: $46.0 billion, or 0.25% of GDP.

of publicly admitting to being a victim of malicious cyber activity are only 3%.[22] In 2016, Thomson Reuters reported 34 new incidents of adverse cyber events experienced by individual U.S. firms.[23] Taking into account the odds of underreporting, this number implies that 1,156 firms have likely experienced adverse cyber events in 2016, which comprises 26.78% of all publicly traded firms.[24] The rest of the estimations proceed as above, but we use the total probability of an adverse cyber event estimated above instead of the 13.85% probability of a material data breach we used earlier.[25] Using this higher probability, we estimate that malicious cyber activity cost the U.S. economy $108.6 billion in 2016, which is 0.58% of that year's GDP.[26]

[22] Ideally, we would like to get a better estimate of underreporting by averaging across multiple observations of known instances of underreporting. In practice, it is very difficult to observe these probabilities based on publicly available information, but we are working on getting additional observations based on government data.
[23] Source: Thomson Reuters and CEA computations.
[24] This number appears large, but it is actually below the 3,000 firms that were notified by the U.S. Government in 2013 that they had been hacked (page 26 of this document).
[25] These probabilities suggest that material data breaches represents roughly half of all adverse cyber events experienced by firms.
[26] When spillover effects are not taken into account, the estimate drops to $87.3 billion, or 0.47% of GDP.

ABOUT THE COUNCIL OF ECONOMIC ADVISERS

The Council of Economic Advisers, an agency within the Executive Office of the President, is charged with offering the President objective economic advice on the formulation of both domestic and international economic policy. The Council bases its recommendations and analysis on economic research and empirical evidence, using the best data available to support the President in setting our nation's economic policy.

www.whitehouse.gov/cea

February 2018