March 2016

Cyber Insurance: A Guide for Policymakers

The market for cyber insurance, a product that did not even exist before the mid-1990s, is booming. According to the Insurance Information Institute, the U.S. cyber insurance market generated about $2 billion in premiums in 2014. Some experts estimate that premiums will increase to $7.5 billion by 2020.[1] High-profile hacks on confidential customer data and prominent companies—like Sony, Target, Apple, multiple large banks, as well as the Department of Defense and U.S. Office of Personnel Management—have raised concerns about the integrity of the personal data entrusted to firms and government agencies. These cyber incidents also raise alarms among policymakers and regulators, who understand that the attacks threaten economic activity, financial markets, and U.S. national security.

In response to these attacks, companies are upgrading their systems and purchasing cyber insurance protection. Government interest is also driving the growth of the market. Nearly all states, for example, now require companies to notify customers of cyber breaches. Cyber insurance is also growing globally, as the European Union is expected to implement cybersecurity rules in the near future. Another dynamic increasing the demand for cyber insurance is the growing realization among directors and officers of companies that they could be held personally liable for cyber attacks.

In this issue brief, the Bipartisan Policy Center's insurance task force starts with the premise that a well-functioning market for cyber insurance, one that offers a robust range of products that meet the needs of consumers in a competitive environment, would benefit consumers, businesses, and national security. Reaching that goal will require overcoming some difficult obstacles. This paper provides a guide to policymakers on how best to address these obstacles and facilitate a well-functioning cyber insurance market in the United States.

BIPARTISAN POLICY CENTER

Background

The recent and anticipated growth in the cyber insurance market is due, in large part, to the growth in cyber attacks. In 2014, there were 783 reported data breaches in the United States, and those breaches exposed 85.6 million records.[2] There were likely many more breaches that went unreported. These attacks carry a significant cost. One report estimated the annual cost of cybercrime to the global economy is between $375 billion and $575 billion per year.[3]

One of the chief obstacles in the further development of the cyber insurance market is defining what constitutes cyber insurance. Among the elements a cyber insurance protection policy can include are:

- Liability for a security or privacy breach, such as when confidential customer information is compromised
- Costs of notifying customers of a breach and providing them support services
- Losses from business interruption following an attack
- Costs for restoring or replacing lost or damaged data
- Liability for directors and officers of a company targeted by an attack
- Costs associated with settling cyber extortion threats

Given these various risks, cyber insurance policies are often customized for individual firms rather than sold as standard policies. Also, since the market is relatively young, policy terms have not been standardized through judicial interpretations.

Obstacles to a Healthy Cyber Insurance Market

The central obstacle to a robust, well-functioning cyber insurance market is the inability of both insurers and insureds to know exactly how much risk is involved in cyber attacks. The difficulty in underwriting cyber insurance means that the supply and demand for insurance coverage may be significantly mismatched to actual risk. If insurers underestimate the risk that they are insuring, they may face heavy losses for one or more insurable events. On the other hand, if they overestimate the risk they are insuring, they may not offer enough insurance to meet demand or offer it at excessive premiums that deter potential customers from purchasing the coverage they need to mitigate risk.

A number of factors contribute to the difficulty in underwriting cyber insurance.

Lack of Data

At a basic level, there is a lack of high-quality data about how many cyber incidents are taking place and how much damage those incidents are causing to firms and the economy as a whole. As noted above, there are some general estimates of the number and cost of breaches, but there is no established mechanism for companies and government agencies to share data with each other. Last year, Congress did enact cybersecurity legislation that should help to address this gap and lead to more data sharing on certain kinds of cyber incidents once the law is implemented.[4]

Yet, the data challenge goes beyond tracking attacks and sharing information. Some companies that are hacked do not realize it and so never report those attacks. Other companies prefer to keep knowledge of attacks private, fearing reputational damage. Still others realize that they were attacked but are not able to fully assess the damage done. In short, the assessments being made today about the scope and significance of cyber risk are educated guesswork.

Difficulties in Threat Modeling

The evolving nature of cyber threats also makes it difficult to assess underwriting risk. Good data about past events that triggered claims gives insurers the opportunity to model the likelihood of future losses. But even if the ability to understand and model past cyber threats improves materially, there will still be uncertainty in assessing future risk because the nature of cyber threats can change so rapidly. A foreign government or activist hacker group could announce it had both a new technology for which there was no defense and a plan to undermine major U.S. corporations. In turn, these events could destabilize financial markets and have a disruptive impact on both insurers and the corporations that may be subject to attacks.

Problems do not arise just from external sources. Many cyber incidents can be traced to employees who either knowingly or unwittingly opened a window to allow an attack. A company laptop that is inadvertently left at an airport can become a tool for hackers. Each time a firm hires a new employee with access to critical systems, its risk profile immediately changes. Managing these internal risks will remain a challenge for companies and insurers.

The effectiveness of modeling will depend on the stability and predictability of the technology used for cyber attacks. If attacks retain a significant degree of unpredictability, then pricing future risk will remain problematic.

Aggregation Risk

The primary problem for insurers to solve may be aggregation risk, or the risk that they will have to pay a large number of unexpected claims within a short period of time due to related losses, such as those that follow an earthquake or hurricane. Insurers are used to focusing on the risks of insuring a specific firm, but they are not as used to focusing on the risks to the entire insurance industry from vulnerabilities that affect many companies at the same time.

An example of this aggregation risk would be if most of the major firms in a sector—such as power utilities or financial institutions—used the same control software, enterprise risk-management strategy, or IT infrastructure. A cyber attack on a vulnerability in any of those systems could affect an entire sector at once, potentially resulting in huge simultaneous losses for the insurance industry. One 2015 report estimated that a major cyber attack on the U.S. power grid could result in $21.4 billion to $71 billion in claims paid by the insurance industry, with a much larger impact on the U.S. economy.[5] In this sense, aggregation risk is systemic risk.

Policymakers have addressed aggregation risk in some other contexts. In response to the terrorist attacks on September 11, 2001, Congress enacted the Terrorism Risk Insurance Act (TRIA) in order to sustain a viable private market for the many parts of the economy that would require terrorism risk insurance. TRIA provides a government backstop for extreme-loss scenarios. Similarly, the federal flood insurance program provides subsidized insurance coverage for homeowners and businesses in flood zones. In contrast to flood insurance, insurance against most other disasters, which also can result in huge, aggregated losses, has largely been sold on the private market. However, the aggregation risk from most disasters can be limited because the damage they cause is generally restricted to specific geographical regions. The same is not usually true of cyber risk.

The lack of quality data on cyber attacks is exacerbated by aggregation risk, which can be difficult to identify and manage. If it cannot be successfully managed, the result could be an insufficient supply of coverage that does not satisfy the needs of the market or a risk of catastrophic losses that the insurance industry cannot handle.

Lack of Understanding of What Is Covered

Even companies that know they need cyber insurance are not always clear on how much coverage they need or are getting. Cyber attacks make one think of virtual damage, but a computer virus can cause physical property damage as well, such as when the Stuxnet virus damaged machinery used in Iran's nuclear program. A firm may believe it is protected by general liability coverage when its policy actually excludes cyber attacks, or the language of the policy is ambiguous and results in denied claims. Some firms may be unaware of the different kinds of losses to which they are vulnerable and only be covered for some of them.

This problem is magnified by the fact that cyber insurance is generally not standardized or sold as a single policy. Coverage is usually tailored to the individual circumstances of specific firms and is cobbled together with different policies that address different kinds of cyber threats. For instance, a company may find it necessary to buy separate policies that address business interruption, customer-response costs, and protection from data loss due to cyber attacks.

The absence of standardized cyber insurance policies also can expose insurers to unanticipated risks. A policy may be deemed to cover losses from cyber attacks simply because that risk is not specifically excluded in the policy. Insurers that sell such a policy may even be unaware of the risk they have taken on with regard to cyber attacks. In 2012, for example, a court ordered AIG to pay almost $7 million in damages to DSW Shoe Warehouse. The court rejected AIG's argument that DSW's crime insurance policy excluded coverage for hacking DSW's computer system.[6] Insurers less well versed in the ins and outs of cyber insurance could find themselves insuring more cyber risk than they realized.

Lack of a Common Vocabulary

The lack of a common vocabulary associated with cyber threats has contributed to the absence of standardized insurance policies. Many of the basic terms related to cyber threats have not been well defined. For example, what exactly constitutes a "cyber incident"? What are "critical infrastructure," "hacking," and "data breaches"? These terms may seem like common sense, but that standard is not good enough when it results in a misunderstanding between a policyholder and an insurer on what precisely constitutes a cyber attack and will trigger a claim.

TRIA policies illustrate this problem. Coverage for cyber attacks under TRIA policies is not settled. TRIA likely does not cover cyber attacks per se, but it likely would cover certain cyber-related damages that would normally be covered by terrorism insurance.[7] Another problem is how to label the attack. Is it "terrorism" or is it a "cyber attack"? The group that hacked Sony Pictures Entertainment in 2014 initially convinced many that the attack was sponsored by North Korea as an act of terrorism, in retaliation for a specific film produced by Sony, but many experts have since questioned that conclusion. It can take years to determine who was behind an attack, and sometimes investigators never know with certainty. Such cases make it hard to know whether the responsibility to cover losses will fall to the insurance industry or to TRIA. It is important not just to develop a common vocabulary, but also one that is adaptable to address uncertain and unforeseen future scenarios.

Disincentives to Share Information

Even though better information sharing on cyber incidents would make it easier to understand and predict future attacks, there are disincentives that push against it. We have listed four of these below.

First, cyber attacks on critical infrastructure and other sensitive targets may be considered national security threats. Releasing information about these attacks could reveal security weaknesses or cause public anxiety or panic. This creates an incentive for officials to avoid releasing information about such attacks, meaning that data on these attacks may be unavailable to policymakers and insurance underwriters.

Second, firms that suffer a cyber attack can sustain damage to their reputations as well as their bottom lines. If customers believe their data will not be secure with a company, they may decide to stop doing business with that company. This reputational risk is another incentive for companies to try to keep cyber attacks as low profile as possible, which creates an incentive to avoid sharing data that would be useful in preventing further attacks and in developing cyber insurance policies.

Third, firms may also fear that the data they share could reveal trade secrets or otherwise compromise their intellectual property if the data are not properly anonymized or if the data were of a kind for which anonymization would be ineffective.

Finally, voluntary data sharing is to some extent a collective-action problem. All stakeholders would benefit from more sharing, but an individual firm has an incentive to take advantage of data shared by others while avoiding sharing its own information.

These examples illustrate why it is so important for the incentive structure for data sharing to be well designed and able to overcome the disincentives to sharing.

Lack of Awareness

Companies are more alert to the threat of cyber attack now than they were a few years ago. However, a significant number of firms are largely unaware of the risk. Some have been the subject of attacks and do not even know it. These firms represent a need for cyber insurance that is not being expressed as demand, which slows the development of the cyber insurance market.

Lack of Resources

Even if small- or mid-sized firms realize they are vulnerable to cyber attacks, they may lack the resources necessary to prevent and respond to such attacks. Also, smaller companies tend to rely more on best practices than on customized solutions to protect themselves. Having fewer resources to devote to protecting themselves makes smaller businesses easier targets for hacking attempts than large enterprises.[8]

Short Claims and Legal History

The claims and litigation history for cyber insurance is thin and offers few guideposts for insurers. Markets for insurance products often develop gradually. This enables insurers to review data on claims and to adjust the features of their products and price them accordingly. Since cyber insurance is a relatively new product, it lacks the claims and litigation history associated with other insurance products. This is a problem that should be solvable over time, but for the moment, it creates further price uncertainty for cyber insurance products.

Difficulty in Assessing Policyholder Efforts

When an insurer evaluates the cyber risk of a firm that wants to buy cyber insurance, the insurer needs to have a good sense of how well the firm is protecting itself from attacks. Does it practice good "cyber hygiene," a set of steps and best practices it can take to prevent attacks? Does it have a good response plan for an attack? Does upper management understand the risk of cyber attacks, and is it committed to prevention?

But it can be difficult for an insurer to evaluate the cyber risk policies and procedures established by a company. For example, an insurer can easily see whether a home has a sprinkler system, smoke alarms, and a security system, and can adjust property insurance rates for the homeowner accordingly. Good cyber hygiene is trickier to evaluate because it involves more subjective assessments that can vary from company to company, such as whether a firm will respond quickly and effectively to an attack, and whether it fully understands its own risk profile. Some insurers offer services, such as assisting firms with prevention and response plans and providing post-attack response services, in addition to policies.

Vulnerability Beyond Company Walls

In an increasingly interconnected world, a company's cyber prevention strategy needs to cover not just its own business and employees, but also its partners and vendors. In 2013, hackers breached Target's customer data by exploiting vulnerabilities at the vendor that dealt with Target's heating and air-conditioning systems. The vendor was connected to Target's networks for billing and contracts, which allowed hackers to indirectly breach Target's security. Further, a single employee at the vendor may have caused the initial breach by being taken in by a fake email that then installed a virus on Target's computer system.[9]

Companies are realizing the extent of such vulnerabilities and have begun requiring vendors and other outside parties to have cyber attack prevention measures and cyber insurance of their own in place.[10] Still, it is difficult to plug every potential security hole and even more difficult to ensure partners and vendors have done so.

Availability and Cost of Coverage

Potential buyers of cyber insurance policies can face a challenge in finding affordable coverage. The supply of cyber insurance has been growing to meet demand, but some companies report not being able to buy coverage for certain exposures, or not being able to buy as much coverage as they would like at prices they can afford. A report from the Treasury Department's Federal Insurance Office (FIO) suggested that the supply of cyber insurance coverage needs to increase to meet demand and that "billion dollar coverage limits are needed to adequately address the losses posed by cyber risks."[11]

The same FIO report pointed to the volatility of cyber insurance pricing as a result of high-profile attacks and the payment of large claims. Breaches and resulting claims payments at a number of retailers has meant that "retailers with point-of-sale exposure have seen 10 to 100 percent increases in primary cyber risk premiums and additional increases in excess layers upon renewal."[12]

To the extent these price increases reflect a better understanding of the risks involved, they are more accurately pricing that risk. To the extent the risks involved are due to a lack of risk awareness or less-than-adequate prevention measures at retailers, they point to the need for significant improvements at these firms.

Government Response

Federal and state policymakers have been acting to address cybersecurity threats as the threat evolves. Below, we mention just a few of those actions.

In late 2015, Congress passed the Cybersecurity Information Sharing Act. That law is designed to provide incentives, including liability protection, for companies to share data with the government on cyber attacks. It also allows the federal government to share unclassified data with other agencies, businesses, and the public. Once implemented, the Act should improve the amount of data available to analyze and model the risk of cyber attacks on. It will be important, however, to monitor and evaluate implementation to assess the new law's impact.

Following the Sony breach, President Barack Obama signed an executive order that declared malicious cyber attacks a national emergency and authorized sanctions against those responsible for such attacks.[13] That order built on the federal government's Comprehensive National Cybersecurity Initiative that had been launched by President George W. Bush in 2008.[14] In 2015, the president followed up on his executive order by directing the creation of a Cyber Threat Intelligence Integration Center to coordinate and analyze intelligence related to cyber threats and incidents.[15] Deputy Secretary of the Treasury Sarah Bloom Raskin has devoted considerable attention to cybersecurity matters,[16] and FIO has convened a series of stakeholder meetings focused on developing underwriting principles for cyber insurance policies and risk mitigation. Since 2013, the National Institute of Standards and Technology has been developing its Cybersecurity Framework of standards, practices, and guidelines to protect critical infrastructure.[17] A number of other federal agencies are developing initiatives to improve cyber hygiene and cyber attack response, as well as mandates to disclose attack information.

The U.S. Department of Homeland Security has held a series of workshops and roundtables that identified three major reasons that cyber insurance offerings remain limited: a lack of actuarial data on cyber incidents, aggregation risk, and the difficulties of modeling cyber threats. These workshops further identified three primary responses to address these issues:

1. A system to share anonymized cyber incident data and make it available in a repository for analysis
2. Tools and models to help insurers better understand the risk cyber attacks pose to critical infrastructure
3. For companies to adopt enterprise risk management programs with buy-in from senior management to address cyber risk[18]

The Department of Homeland Security has followed up on these ideas, including with a 2015 paper recommending 16 categories of data to be included in a prospective cyber incident data repository.[19]

State insurance regulators have also been active in addressing cyber insurance. The National Association of Insurance Commissioners, an organization of state and territorial insurance regulators, created a cybersecurity task force in 2014 that is working to address a range of cybersecurity issues that impact insurance.[20] In addition, nearly all states now require customer notification when companies suffer a data breach.[21] Some in Congress would like to replace the multitude of different state requirements with a single national data-breach notification standard.[22]

The Future of the Cyber Insurance Market

Cybersecurity will only become more important as Americans continue to increase their reliance on connected technologies and as malicious actors see more opportunities to exploit that reliance for economic or political ends. The need for cyber insurance will grow alongside as a necessary element of managing risk.

It is important to consider what form the market for cyber insurance will take. Policymakers and insurers are focused on learning how to adequately understand the risk of insuring against cyber attacks and being able to model the likelihood of future losses.

If these obstacles cannot be sufficiently overcome, some kind of government backstop may be required to cover catastrophic, correlated losses that the insurance industry simply cannot absorb. But the need for such a backstop may only become evident after a truly catastrophic cyber event, which would illustrate in all too visible ways the magnitude of the dangers the country, firms, and individuals face from cyber attacks.

In the absence of such an event, the insurance task force offers the following principles to guide policymakers as they consider how to influence the development of the cyber insurance market:

1. A healthy, competitive private cyber insurance market would improve outcomes for consumers, businesses, and national security. Finding ways to overcome the obstacles on the path to this goal should be the preferred course of action.
2. Improving the collection and sharing of high-quality data on cyber incidents is the most important obstacle to be overcome. Access to better data will help all stakeholders to better understand the risk they are exposed to from cyber attacks, to model the risk from future attacks, and to allow insurers to avoid aggregation risk. Policymakers should find ways to encourage firms to share more data and facilitate its collection, analysis, and sharing with other stakeholders.
3. In general, the cyber insurance market would benefit from greater standardization, such as of terminology, policy language, and best practices for cyber hygiene. There are exceptions to this rule, such as when certain kinds of standardization could increase aggregation risk for insurers.
4. Any legislation considered by Congress to address cyber insurance should be technology-neutral. That is, it should be written to work with existing technologies but also be adaptable to work with future technologies that cannot be anticipated.

These principles will help to develop wise policy for a market that will become much more important in the years to come.

End Notes

1. Robert P. Hartwig and Claire Wilkinson, "Cyber Risk: Threat and Opportunity," Insurance Information Institute, October 2015, p. 2. Available at: http://www.iii.org/sites/default/files/docs/pdf/cyber_risk_wp_final_102015.pdf.

2. Ibid.

3. Ibid., p. 11.

4. "Cybersecurity Information Sharing Act of 2015," S. 754, 114th Cong. (2015) (enacted).

5. Lloyd's and the University of Cambridge Centre for Risk Studies, "Business Blackout: The Insurance Implications of a Cyber Attack on the US Power Grid," 2015, p. 4. Available at: https://www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/business%20blackout/business%20blackout20150708.pdf.

6. Chad Hemenway, "Appeals Court Says AIG Must Pay Retailer's Computer-Hacking Claim," *Property Casualty 360*, September 26, 2012. Available at: http://www.propertycasualty360.com/2012/09/26/appeals-court-says-aig-must-pay-retailers-computer.

7. Hartwig and Wilkinson, Ibid., pp. 9-10.

8. Kate Smith, "Going Viral," *Best's Review*, February 2016, p. 37.

9. Michael Kassner, "Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned," *ZDNet*, February 2, 2015. Available at: http://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/.

10. Hartwig and Wilkinson, Ibid., p. 7.

11. Federal Insurance Office, U.S. Department of the Treasury, "Annual Report on the Insurance Industry," September 2015, p. 67. Available at: https://www.treasury.gov/initiatives/fio/reports-and-notices/Documents/2015%20FIO%20Annual%20Report_Final.pdf.

12. Ibid.

13. The White House, Office of the Press Secretary, Executive Order: "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activity," by President Barack Obama, April 1, 2015. Available at: https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m.

14. The White House, Briefing Room, "The Comprehensive National Cybersecurity Initiative." Available at: https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative.

15. See: The White House, Office of the Press Secretary, "FACT SHEET: Cyber Threat Intelligence Integration Center," February 25, 2015. Available at: https://www.whitehouse.gov/the-press-office/2015/02/25/fact-sheet-cyber-threat-intelligence-integration-center.

16. Sarah Bloom Raskin, "Remarks by Deputy Secretary Sarah Bloom Raskin at the Center for Strategic and International Studies' Strategic Technologies Program," speech, September 10, 2015. Available at: https://www.treasury.gov/press-center/press-releases/Pages/jl0158.aspx.

17. See: National Institute of Standards and Technology, "Cybersecurity Framework," last updated March 1, 2016. Available at: http://www.nist.gov/cyberframework/.

18. National Protection and Programs Directorate, Department of Homeland Security, "Insurance Industry Working Session Readout: Insurance for Cyber-Related Critical Infrastructure Loss: Key Issues," July 2014, pp. 1-2. Available at: https://www.dhs.gov/sites/default/files/publications/July%202014%20Insurance%20Industry%20Working%20Session_1.pdf.

19. National Protection and Programs Directorate, Department of Homeland Security, "Enhancing Resilience Through Cyber Incident Data Sharing and Analysis," September 2015, pp. 1-2. Available at: https://www.dhs.gov/sites/default/files/publications/Data%20Categories%20White%20Paper.pdf.

20. See: National Association of Insurance Commissioners and The Center for Insurance Policy and Research, "Key Issue: The National System of State Regulation and Cybersecurity," last updated January 25, 2016. Available at: http://www.naic.org/cipr_topics/topic_cyber_risk.htm.

21. Hartwig and Wilkinson, Ibid., p. 9.

22. Amy F. Davenport and Norma M. Krayem, "Data Breach Legislation Continues To Be a Congressional Priority," *The National Law Review*, May 11, 2015. Available at: http://www.natlawreview.com/article/data-breach-legislation-continues-to-be-congressional-priority.

BIPARTISAN POLICY CENTER

Founded in 2007 by former Senate Majority Leaders Howard Baker, Tom Daschle, Bob Dole and George Mitchell, the Bipartisan Policy Center (BPC) is a non-profit organization that drives principled solutions through rigorous analysis, reasoned negotiation and respectful dialogue. With projects in multiple issue areas, BPC combines politically balanced policymaking with strong, proactive advocacy and outreach.

bipartisanpolicy.org | 202-204-2400
1225 Eye Street NW, Suite 1000 | Washington, DC 20005

@BPC_Bipartisan
facebook.com/BipartisanPolicyCenter
instagram.com/BPC_Bipartisan
flickr.com/BPC_Bipartisan

BPC Policy Areas

Economy

Energy

Finance

Governance

Health

Housing

Immigration

National Security

About the Insurance Task Force

The Insurance Task Force is part of BPC's Financial Regulatory Reform Initiative, which was created to assess the Dodd-Frank Act and recommend practical policy solutions to improve it. The task force is co-chaired by Republican William H. McCartney, former president of the National Association of Insurance Commissioners and Nebraska state insurance director, and Democrat Robert E. Litan, longtime regulatory policy scholar and former Clinton administration official. Through stakeholder engagement and in-depth analysis, the task force is examining the changing structure of insurance regulation as a result of Dodd-Frank, both within the United States and internationally, and recommending policy reforms that promote effective and efficient regulation for the 21st century.

This paper is the third in a series of mini-papers on current topics in insurance regulation, with more planned for release in 2016. The mini-papers will be followed by a final report of recommendations.

BIPARTISAN POLICY CENTER

1225 Eye Street NW, Suite 1000
Washington, DC 20005

202-204-2400
bipartisanpolicy.org