COUNCIL *on*
FOREIGN
RELATIONS

CYBER BRIEF

Creating a Federally Sponsored Cyber Insurance Program

Robert K. Knake
November 2016

This Cyber Brief is part of the Digital and Cyberspace Policy program.

The U.S. federal government has long debated using insurance as a tool to create incentives for better cybersecurity in the private sector, and has tried to prod the insurance industry to offer cyber coverage. Meanwhile, financial firms and industry groups have pushed the federal government to create a backstop for cyber insurance, arguing that the U.S. government is likely to end up footing the bill should a catastrophic cyber incident occur.

When catastrophes have occurred in other areas, Congress has enacted legislation to repair the damage and made efforts to prevent a similar incident from happening again. This pattern played out following 9/11, Hurricane Katrina, and the 2008 financial crisis, to varying degrees. Anticipating a catastrophic event in cyberspace, Congress should put in place a federal backstop for cyber insurance. Doing so would set expectations for the market and, if constructed properly, reduce the likelihood of a catastrophic cyber event by stimulating the adoption of best practices through insurance requirements and creating incentives to participate in programs that reduce risk for everyone connected to the internet.

BACKGROUND

The Federal Insurance Office estimates that the U.S. market for cyber insurance was as high as $2.75 billion in 2015, as measured in collected premiums. PricewaterhouseCoopers projects that the market will grow to $7.5 billion by 2020. But coverage is far from universal. Despite knowing the risks, most companies are not purchasing cyber insurance. According to a report from Marsh, the world's largest insurance broker, only 15 percent of its clients had standalone cyber insurance, and insurers are quickly working to exclude cyber events from other policies.

Companies that purchase insurance may be subject to high premiums, low limits, exemptions for the types of incidents covered, or all three. Coverage beyond $500 million per incident is currently unavailable on the market; however, the Federal Insurance Office notes that some experts believe that coverage beyond $1 billion is necessary. Moreover, because of the systemic risks posed by cyberattacks, total losses could easily exceed the capacity of insurers to make good on all claims, necessitating government intervention. Lloyd's of London estimates that a cyberattack on the U.S. East Coast power grid could result in $1 trillion in economic losses and $71 billion in insurance industry losses, primarily from business interruption, property damage, and injury or loss of life.

For more than a decade, policymakers have considered whether the threat of such a catastrophic cyberattack could require a federal backstop similar to those established for other risks. Following 9/11, Congress created two programs to address the liability concerns that the private insurance market could not. The Terrorism Risk Insurance Program (TRIP) helped commercial property development recover after the attacks. The Support Anti-Terrorism by Fostering Effective Technologies Act (SAFETY Act) encourages companies to develop antiterrorism technologies that otherwise might not exist because of the small market size and unclear liability if their products failed. Under both programs, the U.S. government must certify an incident as an act of terrorism before a payout is made.

The SAFETY Act has evolved from its initial focus on providing liability protection for technologies such as radiation detectors to providing liability protection for counterterrorism plans for stadiums and other venues. Both TRIP and the SAFETY Act could, in their current forms, provide coverage in the event of a catastrophic cyber incident. Several organizations have proposed expanding the use of the SAFETY Act for cybersecurity.

CHALLENGES TO CREATING CYBER INSURANCE

Federally backstopped cyber insurance could be used to address a series of widely recognized and persistent cybersecurity problems. Currently, too few companies share information on cyber threats, so attackers are more likely to successfully reuse malware, exploit the same vulnerabilities, and use the same methods against multiple companies or organizations. The Federal Insurance Office and other industry reports note a lack of actuarial data as a persistent problem that inhibits insurers from accurately pricing risk. Without sufficient data, insurers will continue to avoid financial risk both by limiting the size of policies and the scope of what they cover.

Although some insurers are amassing data to more accurately price risk for the theft of data such as credit card numbers or personally identifiable information, no company has sufficient information to price risk for destructive attacks. Moreover, insurers do not typically offer premium reductions in exchange for improving cybersecurity practices. This market decision reflects a sad reality for the cybersecurity industry: there is no clear consensus on which cybersecurity practices work and which do not, though some insurers are developing closer relationships with cybersecurity providers in order to access information necessary to accurately price risk. Some technical protocols that can prevent the spoofing of email addresses are only effective if all organizations in a given industry implement them.

Although a federally backstopped insurance program could be used as an incentive to address these challenges, if developed incorrectly, it could displace the private market and leave taxpayers to foot the bill. The National Flood Insurance Program owes the Treasury $23 billion and, in the view of the Government Accountability Office (GAO), has no viable path to repay it based on premiums collected and projected payouts. The GAO estimates that federal crop insurance programs cost taxpayers approximately $8.4 billion a year. Any federal action on cyber insurance should promote the growth of the market, account for systemic risks, and avoid creating a subsidy for predictable cyber events.

RECOMMENDATIONS

A federally sponsored cyber insurance program should use the promise of limited financial liability to promote participation in initiatives that benefit the security of the internet as a whole and reduce systemic risk. Initially, the government's goal should be to use the program to promote the sharing of data on incidents so that insurers can accurately price risk and set premiums. Doing so could provide the data necessary to judge the effectiveness of existing best practices and identify new practices that should be widely adopted.

The federal cyber insurance program should be developed under TRIP, borrowing elements from the SAFETY Act given that, much like terrorist attacks, catastrophic cyber incidents affecting the United States will be rare. TRIP should be expanded to cover cyber events and renamed to allow for coverage of all catastrophic cyberattacks—whether they are carried out by terrorists, state actors, or criminals—including cases in which attribution cannot be determined. The new program should require a minimum level of insurance that must be purchased by participating companies and would cover costs up to a limit, beyond which the federal backstop would come into effect. If calibrated correctly, the program should not undermine the private market for either cyber insurance or reinsurance but should allow insurers to take on additional risk that, in aggregate, might otherwise be unmanageable in the event of a truly catastrophic cyber incident with systemic effects. The net effect of the program should be a larger market than would exist without government intervention.

Although TRIP requires the federal government to certify that an incident was terrorism before a company can obtain a payout, cyber incidents should be exempt from this requirement. The U.S. government has a policy of not publicly attributing incidents unless doing so is deemed to be in its national security interests. Future administrations may wish to maintain flexibility on assigning attribution and thus should not be required to point the finger at a particular actor for the purposes of offering insurance coverage.

Firms seeking to obtain insurance under a federally backstopped cyber insurance program should be required to develop a cybersecurity plan based on guidance from the Cybersecurity Framework, the standard for cybersecurity across industries. The Department of Homeland Security should then certify these plans in a process similar to the SAFETY Act today. Certification could also take place by accredited third party providers. Insurers would be responsible for monitoring implementation of the plan. As part of a minimum standard of care, companies should be required to implement protocols that improve the security of the internet as a whole, such as protocols preventing the spoofing of email addresses used in spear-phishing campaigns.

Participating companies should also be required to share data on the threats facing their network through the federal Automated Indicator Sharing (AIS) program. AIS connects participating companies to an anonymous information network to share indicators of malicious activity. As with other areas of cybersecurity, many companies happily accept indicators but are not motivated to share data on threats targeting their network. Requiring participation in information sharing would strengthen collective defense, raise the cost to a potential attacker, and provide a source of data to inform threat calculations made by insurers.

The federally backstopped cyber insurance program should mandate that companies allow full breach investigations, which include on-site gathering of data on why the attack succeeded, to help other companies prevent similar attacks. This function would be similar to that performed by the National Transportation Safety Board (NTSB) for aviation incidents. When an incident occurs, the NTSB establishes the facts of the incident and makes recommendations to prevent similar incidents from occurring. Although regulators typically establish new requirements upon the basis of NTSB recommendations, most air carriers implement recommendations on a voluntary basis. Such a virtuous cycle could happen in cybersecurity if companies covered by a federal cyber insurance program had their incidents investigated by a new NTSB-like entity, which could be run by the private sector and funded by insurance companies.

Critics will contend that after many years in development, the market for cyber insurance is finally taking off and federal intervention is not required. Yet, though growth rates are impressive, the overall size of the market is small compared to the size of potential losses. Moreover, the market on its own is not producing significant reductions in risk. If carefully developed, a federally sponsored cyber insurance program could significantly reduce the economic risk of a cyberattack, allow the insurance market to more accurately price cyber risk, and encourage the adoption of best practices that can make the internet more secure for everyone over time.

About the Author

Robert K. Knake is the Whitney Shepardson senior fellow at the Council on Foreign Relations. He served from 2011 to 2015 as director for cybersecurity policy at the National Security Council. In this role, he was responsible for the development of presidential policy on cybersecurity, and built and managed federal processes for cyber incident response and vulnerability management. A frequent writer and speaker on cybersecurity, he has been quoted by the *New York Times*, *Wall Street Journal*, and *Washington Post* and has appeared on CNN, MSNBC, and National Public Radio. He holds undergraduate degrees in history and government from Connecticut College and a master's degree in public policy from the Harvard Kennedy School.

The Council on Foreign Relations (CFR) is an independent, nonpartisan membership organization, think tank, and publisher dedicated to being a resource for its members, government officials, business executives, journalists, educators and students, civic and religious leaders, and other interested citizens in order to help them better understand the world and the foreign policy choices facing the United States and other countries. Founded in 1921, CFR carries out its mission by maintaining a diverse membership, with special programs to promote interest and develop expertise in the next generation of foreign policy leaders; convening meetings at its headquarters in New York and in Washington, DC, and other cities where senior government officials, members of Congress, global leaders, and prominent thinkers come together with CFR members to discuss and debate major international issues; supporting a Studies Program that fosters independent research, enabling CFR scholars to produce articles, reports, and books and hold roundtables that analyze foreign policy issues and make concrete policy recommendations; publishing *Foreign Affairs*, the preeminent journal on international affairs and U.S. foreign policy; sponsoring Independent Task Forces that produce reports with both findings and policy prescriptions on the most important foreign policy topics; and providing up-to-date information and analysis about world events and American foreign policy on its website, CFR.org.

The Council on Foreign Relations takes no institutional positions on policy issues and has no affiliation with the U.S. government. All views expressed in its publications and on its website are the sole responsibility of the author or authors.

The Digital and Cyberspace Policy program addresses one of the twenty-first century's most pressing challenges: keeping the global Internet open and secure in the face of unprecedented threats. Through briefings, reports, and the *Net Politics* blog, the program's fellows produce timely analysis on the most important issues in cyberspace. Cyber Briefs are short memos that offer concrete recommendations on cybersecurity, Internet governance, online privacy, and the trade of digital goods and services.

For further information about CFR or this paper, please write to the Council on Foreign Relations, 58 East 68th Street, New York, NY 10065, or call Communications at 212.434.9888. Visit CFR's website, www.cfr.org.