No. 106
March 2012

MERCATUS ON POLICY

IS THERE A MARKET FAILURE IN CYBERSECURITY?

by Eli Dourado and Jerry Brito

MERCATUS CENTER
George Mason University

With more than a dozen related bills in Congress, cybersecurity has become a pressing policy topic. Several of these bills would give federal regulators the power to mandate how private sector networks are secured. But do private networks really need to be told how to protect themselves? If there's no market failure for the government to correct, then shouldn't private networks be left to secure themselves? Having direct knowledge of their systems, they are surely better equipped than outsiders—and should have the greatest incentives—to do so. In this short briefing paper, we explain what a market failure is and how the concept applies to cybersecurity.

WHAT IS MARKET FAILURE?

Just because a threat exists doesn't mean regulation is necessary. If that were the case, Americans would need laws to tell us what kinds of locks to put on our doors. We don't have such laws, of course, because individuals have an incentive to protect their own homes.

If a home is burglarized, it is the resident's belongings that will be taken. In economics jargon, we say that the owner *internalizes* the risk of burglary—that is, he takes it into account. As a result, he will spend an appropriate amount on a lock that matches the risk. Most homes will be well protected with a standard deadbolt from the hardware store. But if a home contains valuable pieces of art, the owner may well choose to go for a stronger lock, an alarm system, and maybe even a guard. If he doesn't and his art is stolen, then he alone *internalizes* the loss.

Proponents of cybersecurity legislation, however, have made the case that private network owners do not completely internalize cyber risks.[1] The reason, they say, is that a loss stemming from a cyber attack—against a financial network, for example—will affect not just the network owner but thousands of consumers as well. Again, in economics jargon, that's called

an *externality*—a cost you don't take into account because it falls on others.

As a result, proponents of regulation say that private network owners won't spend the appropriate amount on security to match the risk. That is a market failure, they say, and only government intervention can ensure that we get the right amount of cybersecurity.

The presence of an externality, however, does not necessarily mean there is a market failure. Externalities are often internalized—again, taken into account—by private parties without government intervention. This is true both generally and in the realm of cybersecurity. Policy makers should, therefore, be careful not to enact cybersecurity legislation just because they observe an externality.

EXTERNALITIES 101

Because cybersecurity legislation is presented as a way to correct externalities, we must understand what exactly externalities are. First, the technical definition: an externality is a cost or benefit that is borne by a party who did not agree to the action that caused the cost or benefit. Externalities that impose costs are called negative externalities, and those that confer benefits are called positive externalities. Now, let's illustrate this concept with some examples.

In the case of home door locks described above, there is no externality because the owner alone internalizes the costs and the benefits of his own actions. Now, let's consider a positive externality. Let's say a homeowner decides to have a garden in front of his house and buys and plants many beautiful flowers. He internalizes the benefits of his actions because he gets enjoyment from his garden, but he doesn't internalize *all* of the benefit. Neighbors and anyone walking past his home will also benefit from the view, even though they did not agree to the owner planting the garden.

A negative externality is just the opposite. Suppose a homeowner neglects his front lawn so that it is overgrown and covered with trash. The result is an eyesore that affects the resale values of neighboring houses. It is a cost imposed on the neighbors without their agreement. In the same way that the homeowner doesn't capture all the value created by his garden, he doesn't capture all the costs his junky front lawn imposes.

In the case of cybersecurity, some experts have argued that network security has positive externalities that private network owners cannot internalize. As a result, they will not provide the "socially optimal" amount of cybersecurity unless the government requires it. This is like saying that we won't see many beautiful gardens unless government mandates it because private homeowners can't internalize all the positive externalities. The economic reality is that just because you recognize that an activity creates an externality, it doesn't mean that there is a *market failure*—that is, that markets left to themselves cannot provide the good. In fact, markets overcome externality problems all the time.

HOW MARKETS DEAL WITH EXTERNALITIES

Government intervention is justified when there is a market failure, and some externalities certainly qualify as market failures. One example is a chemical plant that emits an odorless and colorless gas byproduct that can cause cancer. But not all externalities result in market failures. Policy makers should understand how markets solve externality problems to recognize—as in the case of cybersecurity—when governments should intervene and when they should not. Here are some ways that markets deal with externalities.

In his famous paper "The Problem of Social Cost,"[2] Nobel Laureate Ronald Coase noted that externality problems are reciprocal in nature. For example, say there are two neighboring houses. One of them owned by a writer who needs total silence to do his work, while the other is owned by a violinist whose work is to practice his instrument. The violinist plays six hours a day, during work hours, and while it's not loud, it's somewhat audible inside the writer's home. This is a case of an externality—a positive one if you love violin music but a negative one for the writer. Coase's insight was that to make the violinist stop playing is as much a harm to him as his playing is to the writer.

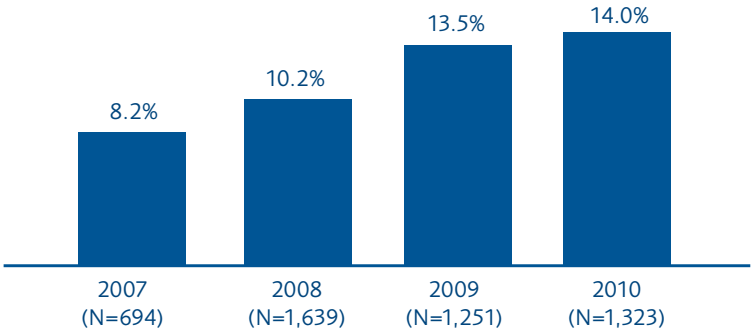
"The real question that has to be decided is: Should A be allowed to harm B, or should B be allowed to harm A?" Coase wrote, "The problem is to avoid the more serious harm."[3]

What Coase discovered is that markets will *automatically* avoid the more serious harm when it is well established who has the right not to be harmed and when it's easy for the parties to transact with each other. Let's say that the socially optimal outcome is that both writer and violinist are allowed to comfortably ply their trades by soundproofing the violinist's studio. Markets will arrive at that outcome—that is, solve the externality—regardless of how you assign the right not to be harmed. If the writer has the right not to be harmed, then the violinist will pay to soundproof his studio. If the violinist has the right, then the writer will pay the violinist to do so.

But what if transacting among parties is more difficult and not as easy as reaching an agreement between two neighbors? A deeper reading of Coase shows that firms can help solve externalities by reducing the cost of transacting. For example, much like some experts argue about cybersecurity today, economists in the past argued that markets would not provide the socially optimal number of lighthouses. Private

FIGURE 1: ORGANIZATIONS ARE STEADILY INCREASING THEIR INVESTMENT IN IT SECURITY

'What percent of your company's IT operating budget will be devoted to IT security this year?'



Base: North American and European enterprise and SMB IT security decision-makers

Source: Forrester Research, Inc. Enterprise And SMB Security Survey North America And Europe Q3 2007, Q3 2008, Q3 2009, Q3 2010.

firms, they said, could not internalize the positive externalities of lighthouses because the cost of transacting with each passing ship would be incredibly high.

When Coase examined the historical record, however, he found that most lighthouses built in Britain in the 17th and 18th centuries were privately constructed. Firms that owned harbors built the lighthouses because many of the ships that benefited from the lighthouse paid for the use of the harbor.[4]

INFRAMARGINAL EXTERNALITIES

Finally, the fact that an externality exists should only matter to policy makers if a government intervention could improve the situation. In many cases, it cannot. For example, when a citizen can read, it benefits all of society and not just the individual. That is a positive externality. As a result, some might suggest that we should subsidize or mandate literacy education.

Just like the homeowner planting a garden, however, it may be the case that learning to read benefits the individual more than it costs. Economists call this type of externality "inframarginal." It means that the homeowner will plant the flowers even if he can't capture all the benefits. As a result, a subsidy or mandate may not be necessary since we will get the same amount of literacy with or without subsidies or mandates.

THE EXTERNALITIES OF CYBERSECURITY

In the case of cybersecurity, the socially optimal level of security is difficult to know. But the best evidence shows that private firms do, in fact, spend quite a bit on securing their assets.[5] As figure 1 illustrates, private firms are devoting larger shares of their IT budgets to security. They do so because they have a lot on the line as well—sometimes billions of dollars. If firms' potential losses are enough to ensure that they take substantial security precautions, then a large portion of the national security externality is irrelevant from a market failure perspective. In other words, private firms may already be providing the positive externality for self-interested reasons and no new subsidy or mandate will make a difference.

CONCLUSION

Policy makers should be careful not to intervene in markets unless they know they can improve the outcome. In particular, they should be sure that a problem exists and that the proposed solution will work. The more they can rely on concrete evidence, the better. Policy makers should also be suspicious of interest groups who benefit from regulation at the expense of everyone else. There is a lot of money to be made by sensationalizing cybersecurity risks, so we need to be wary of these claims.

Regulating externalities when the market has already internalized them is not just unnecessary; it may be harmful. If the government creates regulations for minimum gardening standards because it is concerned about the positive externalities from gardens, people would have to expend time and money to determine whether their flowers are sufficiently beautiful to comply with the regulations. The regulations would make a special interest group out of professional gardeners, who would lobby for higher standards. The government would have to spend money on a garden police to enforce the regulations.

Like gardens, the Internet developed without government intervention. Unnecessary regulation could break down the norms and practices that caused the Internet flourish in the first place.

ENDNOTES

1. CSIS Commission on Cybersecurity for the 44th Presidency, "Securing Cyberspace for the 44th Presidency," December 2008, http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf; U.S. Senate Committee on Commerce, Science, and Transportation, Hearing 111-667, February 23, 2010, Testimony of James A. Lewis, http://www.gpo.gov/fdsys/pkg/CHRG-111shrg57888/html/CHRG-111shrg57888.htm; and Michel Van Eeten and Johannes M. Bauer, "Emerging Threats to Internet Security: Incentives, Externalities and Policy Implications," *Journal of Contingencies and Crisis Management* 17 (December 2009), 221-32.

2. Ronald H. Coase, "The Problem of Social Cost," *Journal of Law and Economics* 3 (October 1960), 1-41.

3. Ibid., 2.

4. Ronald H. Coase, "The Lighthouse in Economics," *Journal of Law and Economics* 17, no. 2 (October 1974), 357-76.

5. For a review of survey evidence concerning the financial sector, see Benjamin Powell, "Is Cybersecurity a Public Good? Evidence from the Financial Services Industry," Independent Institute Working Paper no. 57, March 14, 2005, http://www.independent.org/pdf/working_papers/57_cyber.pdf.

The Mercatus Center at George Mason University is a research, education, and outreach organization that works with scholars, policy experts, and government officials to connect academic learning and real-world practice.

The mission of Mercatus is to promote sound interdisciplinary research and application in the humane sciences that integrates theory and practice to produce solutions that advance in a sustainable way a free, prosperous, and civil society.

Eli Dourado is a research fellow at the Mercatus Center at George Mason University with the Technology Policy Program.

Jerry Brito is a senior research fellow at the Mercatus Center and directs the Technology Policy Program. His research focuses on technology and telecommunications policy, government transparency and accountability, and the regulatory process.