CYBERSECURITY

Companies and consumers are increasingly worried about securing their digital information. A single data breach that compromises a firm's trade secrets or customer information can cost $1 billion or more in identity theft, lost business, system repairs, legal fees, and civil damages. Although cybersecurity is primarily a technological and economic challenge, laws and regulations also shape the choices that firms and individuals make about how to secure their systems and respond to intrusions.

Congress should:

- Reject proposals to regulate private-sector cybersecurity practices.
- Amend federal privacy statutes to remove impediments to the sharing of cyberthreat information among private firms.
- Focus on defending government systems and networks from cyberattacks.

The federal government has two primary roles in cybersecurity. First, it should enforce laws against accessing computers and networks without authorization by investigating suspected intrusions and prosecuting such offenses. Second, it should better secure its own computers and networks—with a particular focus on those systems that could, if compromised, endanger human life.

Some bills introduced in Congress would have the federal government regulate private-sector cybersecurity practices. Those proposals, however, are unwise, for any improvement they bring about in cybersecurity—if one is even realized—would likely be offset by countervailing economic burdens. Although many businesses have experienced costly cybersecurity intrusions, those businesses also tend to bear much of the ensuing costs—customers leave, insurers increase premiums, lawsuits are filed, and so forth.

Firms that suffer cyberattacks because of their lax cybersecurity practices often impose costs—externalities—on third parties who may be unable to recover the resulting losses, such as the time a consumer spends resolving disputes with banks over fraudulent credit card purchases. But the mere existence of that externality does not necessarily merit government intervention to eliminate it. Instead, such regulation is desirable only if it induces firms to take additional cost-effective precautions.

Even if a systematic market failure existed in cybersecurity, assuming that regulators are properly equipped to remedy that failure is folly. Why should regulators be expected to know how a firm should allocate its cybersecurity budget or how much it should spend on cybersecurity? Adjusting liability rules so that companies bear a greater share of the costs resulting from their cybersecurity behavior is far more likely to enhance social welfare than prescriptive regulation.

In addition, Congress could amend several federal laws to improve cybersecurity, albeit perhaps only marginally. For instance, various federal statutes limit the authority of a provider to intercept communications that traverse its own network or to share data that rest on its servers. Although those provisions aim to protect subscriber privacy, they also impede providers' ability to understand cyberthreats and to share their knowledge with other providers. Those statutes do contain exceptions that permit interception and sharing in certain circumstances—for instance, with the subscriber's "lawful consent" or to protect the provider's property—but those exceptions do not go far enough to ensure that contractual arrangements between a provider and its subscriber will suffice to enable interception and sharing.

Therefore, Congress should amend federal law to clarify that companies are generally free to monitor their own networks and systems for cybersecurity threats. To that end, in 2012 and again in 2013, the House of Representatives passed the Cyber Intelligence Sharing and Protection Act to liberalize the sharing of cyberthreat information (CISPA, H.R. 3523 in the 112th Congress; H.R. 624 in the 113th Congress). However, both versions of CISPA afforded companies exceedingly broad liability protection for cyberthreat information sharing, sweeping away not only federal statutes but also state common-law remedies as well.

In reforming federal laws to improve cybersecurity, lawmakers should respect contracts between private entities, some of whom may bargain for information-sharing regimes that differ from the statutory baseline. For that matter, cybersecurity legis-

lation should disavow any preemption of common-law principles—including the sanctity of contract and the duty to abstain from unreasonably causing harm to strangers—so that judges can adapt those doctrines to cyberthreats through case-by-case adjudication.

Experts: Ryan Radia, Wayne Crews

For Further Reading

Jerry Brito and Tate Watkins, "Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy," *Harvard National Security Journal,* Vol. 3, No. 1 (2011) 39–84, http://harvardnsj.org/wp-content/uploads/2012/01/Vol.-3_Brito_Watkins.pdf.

Center for Strategic and International Studies, "Securing Cyberspace for the 44th Presidency," December 2008, http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf.

Eli Dourado, "Is There a Cybersecurity Market Failure," Working Paper, no. 12-05, Mercatus Center, January 2012, http://mercatus.org/sites/default/files/publication/Cybersecurity_Dourado_WP1205_0.pdf.

Richard Epstein, "The Virtues of Simplicity," in *Simple Rules for a Complex World*, 21–36, Cambridge, MA: Harvard University Press, 1997.

Government Accountability Office, "Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented," GAO-13-187, February 2013, http://www.gao.gov/assets/660/652170.pdf.

Tyler Moore, "Introducing the Economics of Cybersecurity: Principles and Policy Options," in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, 3–24, Washington, DC: National Academies Press, 2010, http://goo.gl/dIuPTq.

Paul Rosenzweig, "Cybersecurity and the Least Cost Avoider," *Lawfare* (blog), November 5, 2013, http://www.lawfareblog.com/2013/11/cybersecurity-and-the-least-cost-avoider/.

Ryan Radia and Berin Szoka, "CISPA Shouldn't Infringe on Freedom of Contract," *RedState*, April 16, 2013, http://www.redstate.com/2013/04/16/cispa-shouldnt-infringe-on-freedom-of-contract/.