STATEMENT

of

Paul Rosenzweig
Senior Fellow, R Street Institute
Red Branch Consulting, PLLC
Professorial Lecturer in Law, George Washington University
Washington, D.C.

before the

Subcommittee on Financial Institutions and Consumer Credit
Committee on Financial Services
United States House of Representatives

February 14, 2018

Choosing the Right Cybersecurity Standards

Introduction

Chairman Luetkemeyer, Ranking Member Clay, and Members of the Committee, I thank you for your invitation to appear today and present testimony on the question of data security for financial institutions. My name is Paul Rosenzweig and I am a Senior Fellow at the R Street Institute.[1] I am also the Principal and founder of a small consulting company, Red Branch Consulting, PLLC, which specializes in, among other things, cybersecurity policy and legal advice; a Senior Advisor to The Chertoff Group and a Professorial Lecturer in Law at George Washington University where I teach a course on Cybersecurity Law and Policy. From 2005 to 2009 I served as the Deputy Assistant Secretary for Policy in the Department of Homeland Security.

[1] The R Street Institute is a public policy, research and educational organization recognized as exempt under section 501(c)(3) of the Internal Revenue Code. It is privately supported and receives no funds from any government at any level, nor does it perform any government or other contract work. Information about our funding is available at: http://www.rstreet.org/about-rstreet/funding-and-expenditures/, and my Truth in Testimony Disclosure accompanies this testimony.

My testimony today is in my individual capacity and does not reflect the views of any institution with which I am affiliated or any of my various clients. Much of my testimony today is derived from prior academic work I have done in this field.[2]

In my testimony today, I want to make five basic points, which I can summarize as follows:

- There is good evidence that there is a market failure in the provision of cybersecurity;
- There is less evidence on how best to respond to that through regulation, litigation, tax credit or some other federal program;
- Assuming a regulatory response is chosen, the best structure is one with an emphasis on flexibility and scalability (rather than a more mandatory/top-down version);
- Standards of this sort would have the added virtue of stopping the FTC from regulating by consent decree with all the uncertainties attendant thereto; and
- It will have the implicit effect of a creating a safe harbor – which is a good thing and might benefit from being more explicit.

Market Failure

Recent history is replete with examples of data breaches and the harm they cause. Especially relevant to this committee is the Equifax breach that resulted from poor data security practices (the company failed to apply an available patch) and compromised the sensitive, personal data of over 140 million Americans. Some of the data, like Social Security numbers, cannot be changed meaning that individuals may face a long period of frustration and vulnerability to identity theft. This event was largely preventable had Equifax implemented reasonable security measures such as encrypting relevant data.

The federal government itself has not been immune to cyber-attacks. A few years ago a breach at the Office of Personnel Management compromised records of over 20 million people that also contained sensitive information, such as Social Security numbers and fingerprints. Although it was made public in 2015, the attack occurred more than a year earlier and went unnoticed by OPM.

These attacks are emblematic of the fact that U.S. companies and the U.S. government have been and remain vulnerable to attacks, many of which are by actors linked to nation-states that are adversaries of the United States. Nor are they isolated incidents. As the most recent annual Verizon Data Breach Investigations Report notes, 2016 (the last year for which data is available) saw more than 40,000

[2] *See, e.g.,* Paul Rosenzweig, *Cyber Warfare: How Conflicts in Cyberspace are Challenging America and Changing the World* (Praeger Press 2012); Paul Rosenzweig "Cybersecurity and Public Goods: The Public/Private 'Partnership,'" *in Emerging Threats* (Hoover Institution Task Force on National Security and Law 2011); S. Baker et al., "Regulators in Cyberia," Regulatory Transparency Project of the Federalist Society, July 2017. https://regproject.org/wp-content/uploads/RTP-Cyber-Privacy-Working-Group-Paper.pdf.

incidents and almost 2,000 confirmed breaches.[3] So make no mistake, cyber threats are real, and recent experience has shown that neither the private nor public sectors are fully equipped to cope with them.

The task, then, is to identify an appropriate response. In considering the appropriate scope for government intervention it is useful, initially, to begin with a theoretical model of when governmental activity is warranted. This is not to say, of course, that the theoretical model governs our decision making, but it often serves as a useful guidepost for examining the question.

As a matter of theory and of ideological commitment (born of the independence that are inherent in the foundations of the internet), most private sector leaders will tell you that there is no need for much, if any, government assistance in the cybersecurity market. The only thing they want from the government is more threat and vulnerability information, and then they want it to get out of the way. A closer examination of the theoretical argument suggests, however, that there is some significant room for governmental engagement and, indeed, explains partially, why so many, frequent cybersecurity failures have happened. The theory runs something like this:

A public good is a good that is both non-rivalrous and non-exclusive.[4] In other words, its use by one person does not affect its use by others and its availability to one person means that it is also available to every other person. Public goods have characteristics opposite those of private goods (since, for example, the sale of a shoe to one person both affects its use by others and makes it unavailable to them). The classic example of a public good is national defense. The enjoyment of defense services provided to protect one citizen does not affect the protection enjoyed by another citizen, and defense services provided to one citizen are enjoyed by all other citizens.

Public goods are, typically, beset by two problems – free riders and assurance. Free-riders arise when an individual hopes to reap the benefits of a public good but refuses to contribute to its creation because he thinks others will do so. The assurance problem exists when people refuse to invest in the production of a public good because they believe there will never be enough cooperative investment to produce the good and, thus, that the investment would be futile.

The classic solution to this conundrum is governmental intervention. When a public good is viewed as necessary but cooperation is unavailing, the government coerces its citizens to cooperate through taxation and provision of the public good.

Security in cyberspace, like physical security in the kinetic world, is a market good. People will pay for it and pay quite a bit. But, as in the real world, security in cyberspace is not a singular good – rather it is a bundle of various goods, some of which operate independently and others of which act only in

[3] *See, e.g.,* Verizon Data Breach Investigations Report (DBIR) from the Perspective of Exterior Security Perimeter, July 26, 2017. https://www.verizondigitalmedia.com/blog/2017/07/2017-verizon-data-breach-investigations-report/.

[4] *See, e.g.,* David Schmidtz, *The Limits of Government: An Essay on the Public Goods Argument* (Westview Press: 1991).

combination. Broadly speaking these goods are purchased in an effort to protect networks; hardware; data in transit and stored data from theft, destruction, disruption or delay.[5]

Given the breadth of the scope of the concept of cybersecurity goods, it is unsurprising that different aspects of the bundle may be provided by different sources. Just as some security in the physical world can be purchased directly on the private market, so too in cyberspace many security systems (e.g. anti-virus software and intrusion detection systems) are private goods, bought and sold between private sector actors. They are rivalrous (because their use affects other actors) and excludable (since one can limit their use by other actors). Indeed, evidence from the financial sector suggests that cybersecurity is—to a very large degree—a private good. The question is whether or not it is adequately provided by the private sector.[6]

The answer to that question lies in the conception of externalities. Even if cybersecurity is a private good, this does not mean that government has no role in its production. In many instances, the production of a private good will cause an externality – that is, the activity between two economic actors may directly and unintentionally modify a third-party's cost-benefit analysis.[7] Externalities can be either positive (as when a transaction I voluntarily enter into benefits a third party who pays nothing for the benefit) or negative (when the transaction harms an individual).

Many cybersecurity activities have positive externalities. For example, by securing my own server or laptop against intrusion, I benefit others on the network who are derivatively made more secure by my actions. Indeed, almost every security measure performed on any part of cyberspace improves the overall level of cybersecurity by raising the costs of an attack.[8]

But cybersecurity also has two negative externalities. The first is a diversion effect: some methods of protection, such as firewalls, divert attacks from one target to another, which means that one actor's security improvement can decrease security for systems that are not as well-protected.[9]

The second is a pricing problem: private sector actors often do not internalize the costs of security failures in a way that leads them to take adequate protective steps. When software fails to prevent an intrusion or a service provider fails to interdict a malware attack, there is no mechanism through which to hold the software manufacturer or Internet service provider responsible for the costs of those

---

[5] Eric A. Fisher, *Creating a National Framework for Cybersecurity: An Analysis of Issues and Opinions* 7 (Nova Science Publishers: 2009).

[6] Benjamin Powell, *Is Cybersecurity a Public Good? Evidence From the Financial Services Industry*, 1 J.L. Econ. & Pol'y 497, 498 (2005).

[7] *See* Roy E. Cordato, *Welfare Economics and Externalities in an Open Ended Universe: A Modern Austrian Perspective*, 2 (Kluwer Academic Publishers: 1992) .

[8] *See* Christopher J. Coyne, *Who's to Protect Cyberspace?*, 1 J.L. Econ. & Pol'y 473, 475-76 (2005).

[9] Kobayashi, "Private Versus Social Incentives" *supra*. Less persuasively, Neal Katyal has argued that purchases of private security goods spread fear, thereby potentially increasing the crime rate. See Neal K. Katyal, "The Dark Side of Private Ordering: The Network/Community Harm of Crime," *The Law and Economics of Cybersecurity*, p. 202.

failures. Consequently, the costs are borne entirely by the end users. In this way, security for the broader Internet is a classic market externality, the true costs of which are not adequately recognized in the prices charged and costs experienced by individual actors.

Subsidy, Regulation, or Litigation?

Addressing the dual nature of these cybersecurity externalities poses a significant policy challenge. Both cases suggest a role for government. But identifying which externality predominates is essential, since the two types point to different policy solutions. We typically subsidize private goods that cause positive externalities because not enough of those goods exist and we wish to encourage investment. By contrast, we often tax or regulate private goods that cause negative externalities to compel the original actor to internalize some of the external costs. Doing that forces the private actor to reduce the level of production to one commensurate with its true costs, or it subject failures to meet standards to a litigation or administrative response.

In either case, two broad caveats to government involvement in the private sector's provision of cybersecurity merit note. First, as with any governmental interference in the marketplace, public choice theorists suggest the exercise of great care regarding the government's ability to systematically make the right choices. This is because rent-seeking behavior by an economic actor seeking a regulatory or legislative preference will adversely affect decision-making.[10] They believe subsidies, taxes and regulations will not foster the "right" result, but rather the result that concerted lobbying efforts favor—a concern that is neither unique to cybersecurity nor unfamiliar to this Committee.

Second, the pace of technological change has increased exponentially—a factor that is perhaps unique to cybersecurity. But the government's hierarchical decision-making structure allows only slow progress in adapting to this phenomenon and operates far too slowly to catch up with the change. We make decisions at the speed of conversation, but change happens at the speed of light.

Thus, though one may acknowledge the theoretical ground for government regulation of cybersecurity based on the externalities that exist, one may doubt the government's capacity to exercise its authority in a timely manner– especially when it acts in a mandatory way. Put bluntly, by the time the government closes its notice and comment period and reaches a decision, the technology at issue will likely be obsolete.

Of course, the contrary argument is also quite well-known and equally persuasive. Whenever we have chosen to address a pricing problem through litigation, there are difficulties that have been extensively documented. Principal among these is the significant degree of transactions costs. Operating a civil justice system is expensive and participating in that system is equally expensive, if not more so. These costs, unrelated to the merits of litigation, have a strong tendency to distort the market in ways that are

[10] See Gordon Tullock, "Public Choice," The New Palgrave Dictionary of Economics Online (2d ed. 2008), http://www.dictionaryofeconomics.com/article?id=pde2008_P000240&q=rational%20choice&topicid=&result_number=1.

often unanticipated – sometimes preventing necessary corrective litigation and at other times incentivizing litigation without social benefit.

The second, equally well known problem is that litigation systems tend to accentuate rather than mitigate problems of free-riders and assurance. The benefits from litigation are often randomly distributed rather than used to ameliorate actual injury. And, of course, the attorneys often garner windfall profits for activities with relatively modest social utility.[11]

As such, even though the case for intervention in the cybersecurity market is relatively robust, it is fair to say that the evidence supporting a particular approach to that intervention is modest and that choices among the options are all likely to have unintended consequences.

The Right Approach

All of which leads to a singular recommendation: **First, do no harm.** Approach the problem with actions that take modest steps in the first instance and be willing to revisit settled approaches as we gain empirical experience with the problem. In the end, if a regulatory approach is chosen at all, it should be a flexible, scalable standard-setting approach with a light administrative enforcement mechanism, rather than a hard, mandatory approach with a heavy civil sanction. Here are some principles that should guide our effort:

First, we should avoid recapitulating a "Maginot Line-type" mentality that posits that adequate protection can prevent cyber intrusions. Our efforts must include a consideration for resiliency.

Second, our approach should learn from what we are already doing. For example, NERC now sets cybersecurity standards for the electric industry, and the CFATS program has cybersecurity performance standards for the chemical industry. The hallmark of those programs is that they avoid a "one-size-fits-all" mandate and instead focus on adopting standards of performance that scale to the size of the enterprise.

Third, we must be careful that our efforts do not have adverse effects on Internet governance and our international posture. Cyberspace is a borderless domain and an American regulatory system will not mix well with that structure. Already, China argues that its regulation of the internal Chinese cyber domain is "just like" our use of NIST to set standards. We may comfortably laugh that off now, but we will have a much harder time making the public case for internet freedom if our own security standards run at all in the direction of, say, identification requirements (that is, affirmative log-on systems of positive identity), as they likely will.

Finally, we must develop a system that creates more certainty than it does uncertainty. That requires two things: guidance and reassurance.

[11] *See generally*, Keith N. Hylton, Litigation Costs and the Economic Theory of Tort Law, 46 U. Miami L. Rev. 111 (1991).

As to guidance, we need a model that relies on a flexible standard, but also one that is clearly articulated. By contrast, for example, today much of the guidance from the FTC to consumer enterprises on acceptable cybersecurity practices comes in the form of consent decrees that, taken together, articulate an indefinite standard of reasonable behavior. That is a remarkably poor way to set standards.[12]

In the cyber and privacy sector, the FTC has brought over 200 regulatory enforcement actions. Because of the reputational harm, distraction and cost of litigating these matters, many companies will settle with the FTC and sign a consent decree. Such agreements are not subject to oversight or review by courts. In some consent decrees, the FTC takes the view that it should monitor the company for 20 years. In the life of the information economy, 20 years covers the birth, use and death of multiple generations of a technology.[13]

Additionally, if a company wants to stay out of the FTC quagmire, it will struggle to do so because the FTC has issued very little guidance to articulate what "unfair business practices" means. Indeed, the FTC declines to adopt official guidance that would alert businesses to the sort of conduct that the agency considers unfair. As Judge William Duffey, a judge involved in one of the only two cases that have gone to court challenging the FTC's consent decrees, observed: "how does any company in the United States operate when [it asks the FTC] 'tell me exactly what we are supposed to do,' and you say, 'well, all we can say is you are not supposed to do what you did.' … [Y]ou ought to give them some guidance as to what you do and do not expect, what is or is not required. You are a regulatory agency. I suspect you can do that."[14] Indeed, it is far better to establish a set of rules that defines a standard in statute and allows for enforcement through administrative measures that are subject to judicial and congressional review.

This leads to the second necessary component of any standard-setting exercise: the quality of reassurance. Put simply, no enterprise will invest resources in achieving performance standards without some assurance that doing so is of benefit to the enterprise. Part of the benefit, of course, will accrue from the enhanced safety that (presumably) follows from the adoption of an appropriate standard of care.

But in reality, a major portion of the benefit will lie in the fiscal security of knowing that the enterprise has taken adequate steps to avoid liability for inadequacy. Perhaps that sort of safe harbor will be

[12] For clarity sake I should note explicitly that the FTC example cited here is simply to illustrate an approach I find unhelpful. I am, of course, aware that many of the institutions the committee oversees (banks, credit unions, insurance companies) are expressly exempt from the Federal Trade Commission Act and that the FTC is prohibited under the McCarran-Ferguson Act from playing any role in the business of insurance.

[13] As expressed by Judge Douglas Ginsburg, "The 20-year term seems to be almost certainly inappropriate in high-tech industries with very fast turnover in product design. […] How many iPhones will there be in 20 years? Twenty years of supervision over that kind of evolution strikes me as completely unfounded." Quoted in S. Baker, et al., "Regulators in Cyberia," Regulatory Transparency Project of the Federalist Society, July 24, 2017. https://regproject.org/wp-content/uploads/RTP-Cyber-Privacy-Working-Group-Paper.pdf.

[14] *Id.* The quotation is from a hearing in the FTC's enforcement action against LabMD.

implicit in any standard-setting effort, but it is worth asking the question whether or not an explicit safe harbor might not generate greater uptake. I tend to think it will and that any regulatory or standards-based intervention by the government should be accompanied by a form of verified compliance that is a bulwark against liability and governmental action.

What then should a standard-setting system look like? In many ways, we already have several good models that have been deployed in various federal agencies. The standard setting at NIST, for example, has been a hallmark of a successful effort, characterized by transparency and inclusiveness. The result has been a series of baseline recommendations that are flexible in implementation and scalable in scope depending on the nature of the enterprise. Appropriate standards must not be developed from a hierarchical, top-down perspective, but rather should be the result of a bottom-up approach that recognizes the significant, and often superior, expertise in the private sector.[15]

One final point bears brief mention. As I understand it, the Committee is also considering federalizing data breach notification law. While I am agnostic on the general proposition, one point bears emphasis – data breach notification is not cybersecurity. It is, at best, a second order effort at transparency as a means to foster security, but it does not directly create a safer cyber environment. To that end, I would urge the Committee to insure that its consideration of data breach rules moves in tandem with more substantive and direct consideration of security standards.

Conclusion

We face a wicked problem. Without a doubt, private sector actions will create externalities that the market cannot account for and that cannot be effectively managed by a self-organizing private sector. But the prospect of government action to correct for those externalities raises the same traditional problems of regulatory capture that attend any government endeavor. More fundamentally, precisely because cyberspace is unique in its rapidly changing and path-breaking nature, we face the almost intractable problem of creating policy too slowly to be of any utility. We should neither want to overly diminish the problems nor be sanguine about the capacity to find useful answers. We should, however, approach the problem with a very healthy dose of humility. A flexible, modest, scalable approach is far better than a harsh regulatory mandate and deserves our serious consideration. Ultimately, then, the principal recommendation for government is to treat cyberspace like any patient with an ailment and "first, do no harm."

[15] A less helpful, more mandatory model that should be disfavored was the way in which New York State developed a regulatory framework for financial service companies. *See* Cybersecurity Requirements for Financial Services Companies, 23 NYCRR 500. http://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf.