MERCATUS CENTER
George Mason University
Bridging the gap between academic ideas and real-world problems

ECONOMIC PERSPECTIVES

ECONOMIC PERSPECTIVES: CYBERSECURITY POLICY REFORMS FOR THE 21ST CENTURY

Prepared by Eli Dourado, Andrea Castillo, and Michael Wilt

The United States faces formidable cybersecurity challenges as the role of information technology in business and communication continues to grow. All cyber threats are not alike. A potential lone criminal committing identity theft and fraud requires a much different policy response than the risk of state-backed hackers launching attacks against critical infrastructures. Smart, targeted policy reforms will strengthen our network security by encouraging proactive research and robust defenses to address each type of threat along every potential attack vector.

Those whose property and information are at risk are in the best position to develop, implement, and maintain cybersecurity solutions. A top-down approach to cybersecurity can never successfully identify and prioritize the vast array of relevant factors for achieving effective cybersecurity, especially in view of the rapid pace at which technology develops. Policymakers should focus on reforms that will empower the public to better protect itself. The goal should be to develop a policy environment that encourages proactive research, reporting, and defense while supporting strong encryption techniques. Mercatus Center scholars have identified several policy reforms that would help accomplish these goals.[1]

FOCUS EFFORTS ON REDUCING FEDERAL BREACHES

Federal agencies now experience around 70,000 information security incidents per year.[2] Many of these are caused by basic mistakes like giving administrator access to contractors in foreign countries, not using strong authentication techniques, not applying software updates, and leaving sensitive equipment lying around.

- *Increased cybersecurity spending has not stemmed breaches.* The government is not in a credible position to help the private sector secure itself until it improves its own network security. After years of increasing spending and information sharing among agencies, the federal government's information security incidents continue to rise every year.[3]

- *Systemic problems cannot be resolved by quick fixes*. The federal government's cybersecurity weaknesses are not merely superficial issues that can be quickly resolved in a few short weeks; they are deep, pervasive, and systemic problems resulting from decades of poor information security practices.[4]

- *More of the same federal initiatives will not work*. These weaknesses cannot be solved by creating new offices or agencies. In fact, as of mid-2015, there were at least 62 federal offices that publicize a mission specifically dedicated to cybersecurity.[5] Meanwhile, many have called for these offices to take on a larger role in defending our nation's information systems. It is unclear that these new federal initiatives will be effective when applied to the larger and less familiar information security systems of the entire nation.

- *"Information sharing" is no panacea*. Legislation that aims to encourage private entities to share more data with intelligence agencies by extending legal immunity to corporations is unlikely to meaningfully decrease the number of cyber breaches.[6] Americans' civil liberties and privacy rights are also at risk, since these proposals lack the needed transparency to assure appropriate safeguards are in place. Furthermore, federal agencies are ill equipped to secure the massive datasets that expanded information storage would require, as the 2015 disastrous OPM hack attests.

SUPPORT STRONG ENCRYPTION TECHNIQUES

The first step to improve protection from foreign cyber espionage is to encourage strong encryption that is turned on by default.[7]

- *Weak encryption means weak national security*. Proposals to outlaw certain encryption techniques or mandate government "backdoors" for investigators ultimately works against law enforcement because criminals can also exploit those weaknesses.[8] Strong encryption strengthens both cybersecurity and national security because it also helps protect classified information and systems from unauthorized access. Policymakers should cease the counterproductive "War on Crypto" and instead develop ways to spread and support these technologies.

- *Internet system infrastructure should be open and auditable*. Encouraging the development of an "open hardware" movement—an extension of the open-source movement that has led to software products like the Mozilla browser and the Linux operating system—will result in an Internet infrastructure, both hardware and software, that is open, auditable, and more secure.[9]

REPEAL OR REFORM RULES THAT INHIBIT SECURITY RESEARCH AND ACTIVE DEFENSE

Many outdated policies and legal norms act as counterproductive roadblocks to critical, security-improving research.

- *Research, reporting, and defense should be allowed and encouraged.* Computer engineers are reluctant to report innocently discovered system vulnerabilities, fearing retaliatory lawsuits. Researchers who discover vulnerabilities should have a safe way to report bugs for quick patching.[10] They should be allowed to defend their systems when they are being attacked, while bearing full liability for any damage they cause to innocent parties.

- *Active defense against hackers is necessary.* The Computer Fraud and Abuse Act (CFAA) was intended to stop fraud and abuse, but, instead it is being used to chill legitimate research and self-help. Congress should add a qualified right of active defense to the CFAA.[11] Businesses should be free to use the technological resources at their disposal to protect themselves and their consumers, while being subject to strict liability in the event of unreasonable countermeasures against an innocent party unrelated to the attacker. This change would force those who invoke the right to active defense to internalize the risk of misattributing the source of the attack.

FEDERAL AGENCIES SHOULD AIM TO HELP THE PUBLIC PROTECT ITSELF

Trusting the public by sharing information with us makes economic sense.

- *Federal "zero-day vulnerabilities" should be declassified.* The government has knowledge of many software vulnerabilities that the developer and vendors lack, but it often conceals this knowledge from the public and businesses. More transparent so-called zero-day policies will allow entities to patch vulnerabilities in a timely fashion and strengthen network security.[12]

- *Businesses have incentives to protect their own business.* Companies and firms, on their own, are best able to solve cybersecurity issues because they have the quickest access to information about relevant threats. The best evidence shows that private firms do, in fact, spend a lot of money securing their own assets.[13]

- *Subsidies and mandates are not viable solutions.* Private firms are devoting larger shares of their IT budgets to security. Businesses have a lot on the line, perhaps up to billions of dollars. Private firms may already be providing enough security for self-interested reasons and no new subsidy or mandate from the government will make a difference.

CONCLUSION

Cybersecurity policy should refrain from imposing sweeping, expensive, top-down solutions that could increase rigidities of existing systems. The federal government can better protect American information systems by shoring up its own network vulnerabilities, supporting strong encryption techniques, and reforming laws to encourage security research and reporting, so that the entities best positioned to do so can strengthen their own cybersecurity.

ENDNOTES

1. http://mercatus.org/events/what-should-we-do-about-cyber-attacks

2. http://mercatus.org/publication/poor-federal-cybersecurity-reveals-weakness-technocratic-approach

3. http://mercatus.org/publication/federal-cybersecurity-breaches-mount-despite-increased-spending

4. http://mercatus.org/publication/after-cybersecurity-sprint-material-weaknesses-persist-among-federal-agencies

5. http://mercatus.org/publication/dozens-federal-cybersecurity-offices-duplicate-efforts-poor-coordination

6. http://mercatus.org/publication/information-sharing-no-panacea-american-cybersecurity-challenges

7. http://mercatus.org/expert_commentary/giving-government-backdoor-access-encrypted-data-threatens-personal-privacy-and

8. https://readplaintext.com/america-s-schizophrenic-anti-encryption-cybersecurity-strategy-2d10375a982

9. http://mercatus.org/expert_commentary/let-s-build-more-secure-internet

10. https://reason.com/archives/2015/08/11/economics-of-the-zero-day-sales-market

11. http://mercatus.org/publication/active-defense-overview-debate-and-way-forward-guardians-of-peace-hackers-cybersecurity

12. http://www.usnews.com/opinion/economic-intelligence/2015/10/19/congress-wont-improve-cybersecurity-under-cisa

13. http://mercatus.org/publication/there-market-failure-cybersecurity

CONTACT

Robin Bowen, 703-801-1344, rbowen@mercatus.gmu.edu
Mercatus Center at George Mason University
3434 Washington Blvd., 4th Floor, Arlington, VA 22201
www.mercatus.org

ABOUT THE MERCATUS CENTER

The Mercatus Center at George Mason University is the world's premier university source for market-oriented ideas—bridging the gap between academic ideas and real-world problems.

A university-based research center, Mercatus advances knowledge about how markets work to improve people's lives by training graduate students, conducting research, and applying economics to offer solutions to society's most pressing problems.

Our mission is to generate knowledge and understanding of the institutions that affect the freedom to prosper and to find sustainable solutions that overcome the barriers preventing individuals from living free, prosperous, and peaceful lives.

Founded in 1980, the Mercatus Center is located on George Mason University's Arlington campus.
www.mercatus.org