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

RESEARCH SUMMARY

WHY THE CYBERSECURITY FRAMEWORK WILL MAKE US LESS SECURE

Many policymakers believe that the increasing economic prominence of online activity has made government-led, centralized cybersecurity standards necessary to protect the nation's critical infrastructure from digital vulnerabilities. The resulting plan, a voluntary federal diagnosis and reaction system called the "Cybersecurity Framework," could actually do more harm than good, according to Eli Dourado and Andrea Castillo of the Mercatus Center at George Mason University.

Cybersecurity Framework proponents ignore—and risk undermining—the sources of dynamic cybersecurity provision that have adequately protected online activity for years, their study says. Incentives already exist encouraging online parties to voluntarily and proactively monitor, publicize, and target destructive online activity. As a result, businesses, consumers, and organizations have safely transacted and collaborated online for decades with few disruptions despite the lack of government involvement.

Even if the Cybersecurity Framework remains voluntary, it threatens to undermine dynamism in cybersecurity and Internet governance, and could promote rent-seeking and corruption. Instead, the government should foster continued dynamic cybersecurity efforts through the development of a robust private-sector cybersecurity insurance market.

For the complete study, see "Why the Cybersecurity Framework Will Make Us Less Secure."

KEY POINTS

The Cybersecurity Framework's Shortcomings
The framework replaces the creative process of trial and error with a one-size-fits-all incentive: compliance with recommended federal standards. This approach has several flaws.

- Cybersecurity threats are always changing and can never be fully represented by even the most expertly designed flowcharts. By prioritizing a set of rigid, centrally designed standards, policymakers are neglecting potent threats that are not yet on their radar.

- The framework's jurisdiction is far too broad, using a definition of "critical infrastructure" that encompasses a wide range of firms and industries. Labeling everything as "critical" causes the classification to lose meaning.

For more information, contact
Bob Ewing, 703-993-4960, bewing@mercatus.gmu.edu
Mercatus Center at George Mason University
3434 Washington Boulevard, 4th Floor, Arlington, VA 22201

- The federal government's own experience with cyber-threat notification processes is abysmal. Agencies routinely suffer data breaches, and mandated cybersecurity procedures—when developed—are rarely followed and show few benefits. If the federal government cannot oversee adequate cybersecurity for itself, it is unlikely it can do so for the whole country.

- The Cybersecurity Framework does not end the federal government's inconsistent practice of overclassifying cyber threats. Until cyber threats are adequately declassified and shared, firms and networks will be in the dark about possible attacks.

- The framework opens the door for rent-seeking and corruption. The parties identified to develop and implement the framework harbor clear conflicts of interest. The framework will add to the number of avenues through which corporations can extract public wealth for private gain.

A Better Solution: Retain and Strengthen Dynamic Cybersecurity

Promoting private cybersecurity insurance is a better way for the federal government to enhance cybersecurity coverage and preparedness for critical infrastructure, such as public utilities and transit systems.

- Cybersecurity insurance can provide competitive coverage for cybersecurity breaches that is tailored directly to the unique needs of each industry and organization.

- Cybersecurity insurance would promote proactive risk reduction efforts to decrease insurance company costs. Insurance companies would use audits and rate pressure to encourage clients with substandard security practices to improve.

- As a spillover effect, insurance companies would learn best practices from experiences with their clients and could continually improve the net level of cybersecurity by developing better recommendations and standards.

- Cybersecurity insurance would more accurately price and distribute risks and liabilities.

RECOMMENDATIONS

Despite the attractiveness of a cybersecurity insurance solution, the market has struggled to adequately expand due to information asymmetries and unclear risk pricing. A first mover with deep pockets and a strong desire for cybersecurity insurance is needed to break this disequilibrium, and one obvious candidate is the federal government. Federal agencies could stimulate the development of a cybersecurity insurance market through a competitive bidding process for beneficial insurance coverage and reasonable premiums from private insurers. This would kickstart the critical risk analysis process and enable insurers to derive needed information and develop best practices.

The federal government should also establish a narrower definition for "critical infrastructure," and remove barriers to the dynamic development of cybersecurity provision for critical infrastructures by declassifying information about known cyber threats. These steps will help improve cybersecurity protection for critical infrastructure and general systems alike. By encouraging emergent solutions, the federal government could help improve the dynamic fabric of our cybersecurity ecosystem. The Cybersecurity Framework threatens to undermine this largely functioning system by imposing a brittle, technocratic standard that benefits specific interests and diminishes the incentives for cybersecurity innovation.