R Street

Free markets. Real solutions.

R SHEET ON

BUREAU OF CYBER STATISTICS

June 2021

BACKGROUND

A dearth of information can translate to faulty strategic decisions in organizational cybersecurity. If managers lack accurate information on where cybersecurity controls are insufficient, they will not know where to invest— or if they are investing too much in one security area.

While cybersecurity is commonly discussed in qualitative terms, some industry leaders, such as Bobbie Stempfley, argue that we need metrics to better understand cybersecurity as an evolving threat landscape. There is also increasing political consensus regarding standardizing measurements, including the existing National Institute of Standards for Technology (NIST) framework, and New York State's cybersecurity framework for insurance companies. While these standards are useful for unification at the institutional level, they focus on guiding rather than measuring security. Too many standards across separate organizations can diminish applicability, especially if they are interpreted differently by security teams.

CURRENT DEBATE

Creating a standardized model of information metrics in cybersecurity requires attaching numerical values to inherently qualitative security characteristics. This presents a challenge in centrally disseminating standardized data. To this end, the Cyberspace Solarium Commission's 2020 report includes Recommendation 4.3: the creation of a Bureau of Cyber Statistics (bureau), "charged with collecting and providing statistical data on cybersecurity and the cyber ecosystem to inform policy making and government programs subsequently informing cyber policymakers with comprehensive and contextual data."

The creation of a bureau raises fundamental questions. Most federal statistic bodies live within the Statistical and Science Policy Office of the Office of Information and Regulatory Affairs under the Office of Management and Budget. According to the Solarium Commission's report, the bureau should reside in the Department of Commerce and work closely with the NIST. But other key relationships, such as that of the bureau with the nascent National Cyber Director, are not yet clearly defined.

SUMMARY

- There is currently no quantitative standard to measure the country's evolving cybersecurity posture.
- The creation of a Bureau of Cyber Statistics would standardize metrics and provide contextualized statistics to policymakers.
- While not all details on the bureau's structure are finalized, Congress should set the bureau in motion by mandating its inception through legislation.

To disseminate relevant information to stakeholders, the bureau would have to receive, store and process sensitive data from organizations. This could include an enterprise's average incidents per year, costs of incidents or mean times to recover from an incident. The bureau could implement a voluntary data collection scheme, financial incentive, mandate, or a combination of these to collect data. However, this is subject to change with ongoing debates surrounding a national data breach law, following Solarium recommendation 4.7.1. It is unclear, for instance, if cyber insurance companies would eventually establish a symbiotic relationship with a bureau by both receiving information and reporting incidents.

ACTION ITEMS

A Bureau of Cyber Statistics would create an analytic body that ameliorates information disparities in the cyber landscape, contributing to a more accurate picture of the country's cybersecurity and helping decision makers to better protect assets. Congress should enact legislation to create such a bureau. The legislation will need to allocate sufficient resources to the bureau to enable functionality.

It should also provide the bureau with adequate authority to achieve its mandate of measuring cybersecurity across the country.

As an initial matter, the bureau should focus on the development of a common lexicon of metrics; it should aggregate existing, disparate data sets. The bureau should also begin by examining the security of government networks, with the expectation that lessons learned from that exercise will be applicable to the measurement of private sector security.

To be a technologically literate agency, the bureau should continually partner with industry leaders and academic researchers. Once implemented, the bureau's output should be relied upon for accurate, data-driven cybersecurity decisions by all stakeholders—including the private sector, the public sector, academia, individuals and others.

CONTACT US

For more information on this subject, contact the R Street Institute, 1212 New York Ave. NW, Washington, D.C. 20005, 202-525-5717.

Sofia Lesmes
Research Associate,
Cybersecurity and Emerging Threats
slesmes@rstreet.org

Paul Rosenzweig
Resident Senior Fellow, Cybersecurity
and Emerging Threats
prosenzweig@rstreet.org