Hashed & Salted | A Privacy and Data Security Update
June 2023

US National Cybersecurity Strategy Prompts Questions and Debate Over What's Next

While the business world has been wrestling with cybersecurity issues for decades, the United States government has not always had a central federal cybersecurity strategy. In March the U.S. government released its latest National Cybersecurity Strategy.

So ... how did they do?

The Key Elements of the National Cybersecurity Strategy

The strategy itself comprises a 39-page central strategy document and a shorter, more focused fact sheet. These documents articulate a few key goals:

- **Protecting Critical Infrastructure.** The government committed to work with private-sector partners to enhance the cybersecurity of critical infrastructure industries such as energy, transportation, financial services and health care.
- **Securing Federal Networks.** The federal government pledged to prioritize the security of its own networks and systems, including enhancing the security of the supply chain for information technology products and services.
- **Strengthening the Cybersecurity Workforce.** The federal government pledged to work with academic institutions and the private sector to enhance cybersecurity education and training programs.
- **Promoting International Cybersecurity.** The government pledged to cooperate with international partners to promote the development of international norms and standards for cybersecurity as well as to enhance cooperation and information-sharing to combat cyber threats.
- **Enhancing Cyber Incident Response.** The federal government pledged to develop and implement national cyber incident response plans, improve coordination and information-sharing among government agencies and the private sector, and enhance the use of advanced technologies for incident detection and response.

Decoding the Significance of the Strategy

- **Federal Promises Are Not (Usually) Empty.** The strategy is premised on a lot of promises but few concrete measures. These promises have their own weight, however, and the entire federal government will have to reorder its priorities to emphasize these specific promises. Where an agency might have blithely ignored a request to share information in 2022, it must now have a plan. The federal government is a huge entity, and getting all of it moving in the same direction on cybersecurity, even slowly, can have a huge cumulative effect. In this way, "mere" promises can be very important.

Attorney Advertising

- **The Big Rebalancing.** It is not reasonable to expect end users to manage their own cybersecurity. As stated in the strategy, "Individuals, small businesses, state and local governments, and infrastructure operators have limited resources and competing priorities, yet these actors' choices can have a significant impact on our national cybersecurity. A single person's momentary lapse in judgment, use of an outdated password or errant click on a suspicious link should not have national security consequences. Our collective cyber resilience cannot rely on the constant vigilance of our smallest organizations and individual citizens."

  The strategy indicates that the United States must "ask more of the most capable and best-positioned actors" in society and that cybersecurity "must be the responsibility of the owners and operators of the systems that hold our data and make our society function, as well as of the technology providers that build and service these systems." The strategy also recognizes that the U.S. government's role in providing cybersecurity has distinct boundaries, including protecting its own systems and networks, ensuring that the private sector does its part to protect itself in cyberspace, and carrying out core governmental functions that support cybersecurity.

- **Proposed Cyber Liability Shifting.** The strategy calls for legislation that would prohibit providers from fully disclaiming liability for vulnerabilities, while providing a safe harbor for companies that follow secure development and maintenance practices. This proposed legislation would precipitate huge changes in how cloud-services providers and their customers apportion responsibility for the security of the cloud platforms. Cybersecurity companies appear to support shifting this liability. While this proposal requires actual legislative acts to have any teeth, it is important to track it closely.

- **Possible New Cybersecurity Requirements for Some Critical Infrastructure Sectors.** At least some private-sector operators of critical infrastructure may soon face new or strengthened cybersecurity requirements under existing regulatory authority. Following the 2021 cyberattack against Colonial Pipeline, the Transportation Security Administration exercised its more than 20-year-old authority to regulate pipeline cybersecurity and issued mandatory cyber directives for the first time. Other agencies may follow suit. Hopefully, the strategy's express desire to harmonize these rules will not result in a regulatory thicket of overlapping and contradictory requirements.

- **Increasing the Importance of CIRCIA.** Efforts to enhance and regulate the cybersecurity of critical infrastructure industries are likely to build on the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) and forthcoming implementing rules from the Cybersecurity and Infrastructure Security Agency (CISA). For example, CISA rules and CIRCIA could be used to require companies to adopt certain cybersecurity frameworks or standards. CISA rules and the National Institute of Standards and Technology's (NIST) Cybersecurity Framework could soon affect a wider array of companies.

- **Know-Your-Customers Rules in the Cloud.** Cybercriminals often utilize fake identities to create cloud accounts, pay for cloud services with stolen payment cards, quickly create and then delete virtual servers used for their attacks, and take other steps to operate cloud-based infrastructure-as-a-service (IaaS) technologies to maintain their anonymity. The strategy directs the secretary of commerce to propose "know your customer" rules requiring IaaS providers to collect information about foreign users' identities and payment, among other data. IaaS providers likely would have to collect an enormous amount of data.

- **New Cybersecurity Requirements in Government Contracts.** The strategy calls for the federal government's procurement system to drive changes in cybersecurity practices and norms. Mechanically, various amendments to the Federal Acquisition Regulation and its supplements could be utilized to standardize cybersecurity requirements in government contracts and require reporting of cyber incidents by contractors, among other requirements.

- **Disrupting and Dismantling Threat Actors.** Often companies can feel alone in combating cybercriminals. The strategy endorses an aggressive approach to disrupting threat actors in cyberspace. For example, it says that "[d]isruption campaigns must become so sustained and targeted that criminal cyber activity is rendered unprofitable and foreign government actors engaging in malicious cyber activity no longer see it as an effective means of achieving their goals." The strategy even goes so far as to explicitly direct the use of military power for such disruption where appropriate.

- **Federal Privacy and Security Legislation.** The strategy stands in favor of federal privacy legislation as well as federal security requirements based on NIST guidance and standards. We will see what effect, if any, that support will have on the federal legislative process.

The strategy is a significant departure from past practices and precedent. Its public calls for regulation, the imposition of liability for insecure software products and services, and the increased involvement of the U.S. military in support of private-sector cybersecurity will not happen quickly or easily.

A very interesting debate over cybersecurity policy is about to begin. Who should bear the cost? Who should share what with whom? What is most important? How do we fight back? These questions are not answered by the strategy, but they are being asked earnestly for the first time. Let's get to work on the answers.

Related Professional

Christopher A. Ott . . . . . cott@loeb.com

7296 REV1 06-13-2023