MARCH 2022

A Shared Responsibility

Public-Private Cooperation for Cybersecurity

By Eugenia Lostri, James Andrew Lewis, and Georgia Wood

Executive Summary

Cybersecurity is a priority for Congress and for the Biden administration as online crime and espionage reach unparalleled heights. To improve cybersecurity in federal agencies and in critical infrastructure, the administration has built a strong team, elevated the positions of White House officials dealing with the issue, and released a series of policy directives. In Congress, 157 pieces of legislation addressing cybersecurity were introduced during 2021, with proposals ranging from capacity building and workforce development to updating federal policy.

Crime and espionage have made cybersecurity a national priority, and action on cybersecurity is more likely than ever in 2022. CSIS convened two private roundtables with senior government officials and senior information security executives from major enterprises in a range of U.S. industry sectors. The goals of the roundtables were to identify common challenges, discuss best practices, and outline avenues for cooperation.

Based on those conversations, roundtable participants identified the following areas of work to improve cybersecurity:

- **"Too many organizations—public and private—are falling short in basic things."** We need to emphasize how effective basic cybersecurity measures can be. We should address the reluctance to implementing basic cybersecurity measures and promoting harmonized standard of care. **"Basic mistakes are being exploited."**

- **"It's the SMBs [small and medium-sized businesses] who struggle the most."** Some reports estimate that more than 40 percent of 2021 cyberattacks targeted small and medium-sized businesses. Developing incentives and providing resources can help SMBs prioritize cybersecurity; **"We have to pull the smaller companies up."**

- **"If a system has 10 million vulnerabilities, many just chip away at patching those slowly."** It's impossible to stop all threats and trying to is a bad way to plan. Protecting the "crown jewels" and accepting some level of vulnerability for other assets is more effective.

- **"The market has not driven security."** If there is no market demand for basic cybersecurity, then there is little incentive for companies to make security the default. The government should leverage its acquisition power to create a higher cybersecurity standard for products and services. **"Government can create carrots to enter its market."** The federal government can use its procurement to require security improvements in the software and tech that everybody uses.

- **"There should be an option of helping and supporting instead of regulating and being adversarial."** The government's attitude during a cyberattack can sometimes be perceived as punitive. It is crucial to strike the right balance between mandatory requirements, penalties, assistance, and incentives, while taking into account sector and company needs. Creating a federal response model that provides victims with the people, resources, and tools they need during and after a cyberattack can help.

- **"There is something the government can do to create the right talent."** Programs that address the cybersecurity workforce gap need to emphasize diversity. A cyber version of the Peace Corps could shape a national push to increase the cybersecurity workforce.

- **"Make sure you are not just sharing information back and forth, but working side by side, either in a virtualized environment or live."** Information sharing and partnership need to be operationalized. If companies don't share information about the threats they face, that can undermine the entire environment. Promoting information and resource sharing across industries can help cement trust between companies, as well as between the public and private sectors. **"Information sharing has to be actionable."**

- **"We have not done a great job working with allies and arresting bad guys."** Timely and effective transnational collaboration between law enforcement agencies and national computer emergency response teams (CERTs) can raise the cost of conducting malicious cyber actions.

The roundtable discussions were not technical in nature. Participants were practitioners and senior managers who have thought strategically about cybersecurity and can put cybersecurity practices into the context of how they affect business models and plans, what practices should be sector-specific, and which should apply broadly.

Some themes from this conversation were not new. These include accelerating efforts to expand the cybersecurity workforce and to build on partnerships (like the Joint Cyber Defense Collective, or JCDC) to create a common threat picture. The need to improve cyber hygiene came up repeatedly—it's not that organizations don't know what to do to achieve better cybersecurity, it's that many still aren't doing it—but there was a recognition that market incentives may not always align with hygiene. One change in the conversation was a greater openness to some mandatory cybersecurity measures, as long as these can avoid being punitive.

A Shared Task

Participants recognized that it is unrealistic to expect the government to stop all attacks, but there are things in cybersecurity that only the government can do. A national strategy for cybersecurity should recognize and leverage comparative advantages and avoid the duplication of efforts. Cooperation requires a shift in mindset, moving from mere event response to the prioritization of prevention. Building resilience is critical. The federal government can benefit from awareness and visibility into cybersecurity risks across U.S. networks provided by companies, and companies can benefit from advisories, resources, and notifications of potential and existing threats provided by the Department of Homeland Security (DHS).

The 117th United States Congress has been active. A total of 157 pieces of cybersecurity legislation were introduced in 2021, focusing on a range of topics, from workforce development to capacity building. A list of these bills can be found here. Many of the bills focus on organizational matters—from establishing processes for cooperation and information sharing to initiating cybersecurity programs.

The Biden administration is prioritizing cybersecurity, taking a three-pronged approach that covers (1) modernizing cyber defenses, (2) ramping up international activity, and (3) ensuring the United States is better positioned to compete in cyberspace.

This has been reflected in the senior cyber positions within the administration. First, fiscal year (FY) 2021's National Defense Authorization Act (NDAA) established the Office of the National Cyber Director (ONCD) within the Executive Office of the President. A staff of approximately 75 is planned to join the first national cyber director, senate-confirmed Chris Inglis, to serve "as a principal advisor to the President on cybersecurity policy and strategy, and cybersecurity engagement with industry and international stakeholders." This position complements the new deputy assistant to the president and deputy national security advisor for cyber and emerging technology in the National Security Council (NSC). Currently held by Anne Neuberger, the new NSC position is responsible "for coordinating the federal government's cybersecurity efforts." Additionally, the Cybersecurity and Infrastructure Security Agency (CISA), headed by Jen Easterly, plays an expanded role in leading the efforts to "strengthen the security, resilience, and workforce of the cyber ecosystem." Chris DeRusha, an experienced cybersecurity expert, serves as both the federal chief information security officer at the Office of Management and Budget and the ONCD's deputy national cyber director. The Department of State is creating a new bureau for cyberspace and digital policy, headed by an ambassador-at-large, that will include the existing Office of the Coordinator for Cyber Issues.

Some participants worried that coordinating among all these offices could prove challenging. However, senior officials have reiterated their close working relationships. The strategic intent statement from the ONCD outlines cooperation and coordination across the stakeholders responsible for cybersecurity, and Director Inglis has explained how all these positions complement each other, saying this work needs to be aligned with the private sector. Director Inglis recently built upon this statement, calling for a revised cyber social contract that emphasizes the role of companies in distributing the burden of cyber defense and the role of the government in providing vital threat information while moving toward true public-private collaboration. Improving cybersecurity requires government and private-sector action. The United States can promote cybersecurity in the private sector through a blend of incentives and mandatory requirements. Executive orders, national security memoranda, and agency directives are creating a strong baseline.

Workshop Findings and Recommendations

Building on different perspectives, roundtable participants identified needs, capabilities, and expectations for improved cybersecurity. The following recommendations align policy with real-world cybersecurity practices.

RAISE THE FLOOR FOR CYBERSECURITY

1. **Promote Best Practices**

Participants reiterated how effective basic cybersecurity measures can be in preventing and mitigating cyber threats. Many attacks succeed because of a failure to observe basic cybersecurity measures, like patching (despite "patch fatigue") or using multi-factor authentication (MFA). Many companies still fail to implement these basic measures. The question, then, is how to decrease this reluctance. There are already frameworks, standards, and principles, but a harmonized standard of care could allow cybersecurity teams to work on value-added items such as threat hunting, instead of things such as auditing firewall rules. Standards of care help direct the priorities of a company.

The National Information Assurance Partnership (NIAP) program offers a precedent for establishing minimum standards. Under NIAP, cybersecurity software being used in the Department of Defense (DOD) was tested prior to deployment. Although it was expensive, it had some success. Requiring some level of quality assurance would be comparable to having to obtain a driver's license or getting Food and Drug Administration approval.

The National Institute of Standards and Technology (NIST) cybersecurity framework, a product of joint work by private- and public-sector organizations, offers a solid guide to cybersecurity. Even if its application remains voluntary, the framework can still shape a company's behavior. The Federal Trade Commission (FTC), for example, argues cases by examining whether a company observes proper procedures as outlined in the framework. For example, in FTC v. Wyndham, the agency alleged that Wyndham Worldwide Corporation had failed to follow proper incident response procedures, "leading to the compromise of more than 619,000 payment card account numbers and more than $10.6 million in fraud loss."

Creating a widely agreed-upon set of principles or standards could help set goals in specific terms. A baseline agreement on security practices across sectors could also inform legislative and executive branch expectations for the private sector. This would build on the NIST framework and the May 2021 Executive Order on Improving the Nation's Cybersecurity to identify what "good" looks like for cybersecurity—something that exists only in a fragmentary and incomplete fashion now—and create specific expectations for company and agency behavior. Some of these best practices need to be mandatory but in other cases, new incentives would achieve better results. If companies can accomplish the basics, then they can address the more complicated threats.

The private sector plays a crucial role. For example, in October 2021, Salesforce, Google, Okta, and Slack announced a Minimum Viable Secure Product (MVSP)—"a set of minimum security requirements for business-to-business software and business process outsourcing suppliers." While MVSP is designed to reduce the risk from outsourcing operations to third-party vendors, it provides a useful model for ways in which the private sector can contribute enterprise-ready products and services.

2. Support Small and Medium-Sized Businesses

SMBs struggle to implement many cyber hygiene measures since they often lack both resources and personnel. Finding the resources for proper cybersecurity is prohibitively costly for many SMBs, and even big companies struggle with this issue. Further, size does not necessarily make a company more or less of a target; some reports estimate that 43 percent of cyberattacks in 2021 targeted SMBs. According to CISA, these companies are tempting targets since they hold data that cybercriminals find valuable and do not usually have strong cybersecurity programs in place.

Limiting the work to the companies with substantial security organizations leaves out a large part of the community. Information sharing between companies, especially from the larger players to SMBs, can help prevent cyber incidents (see finding 8).

Lack of awareness, technical capacity, and resources leaves SMBs trailing in the implementation of measures, undermining the overall environment. Creating the right incentives can help SMBs prioritize cybersecurity. One example would be creating programs where SMBs receive better terms for loans if they reach a minimum security standard (like using MFA).

The provision of specific and tailored resources by agencies like DHS would also help. There are already good models in place: CISA offers a range of resources, including the Cyber Essentials program that shows companies how to implement basic security measures to guard against common cyberattacks and a small business-specific toolkit to help identify and address risks. The United Kingdom's National Cyber Security Centre provides specific advice and resources tailored to organizations without dedicated cybersecurity teams.

Governmental seals of approval or lists of trusted and verified providers can also help SMBs trying to identify and implement the best solutions. The government can play a validating role, simplifying the process and ensuring SMBs can trust their cybersecurity vendors. In the United Kingdom, the Cyber Incident Response network, offered at both the small and medium-sized enterprise and large enterprise levels, certifies companies that can help organizations after cyberattacks.

3. Protect the Crown Jewels

Prioritizing and setting mandatory requirements for basic cybersecurity measures would improve cyber resilience. Raising the bar for general cybersecurity and the implementation of basic cyber hygiene measures is laudable, but a realistic approach also needs to recognize that stopping all threats is impossible. Some actors—those with more sophistication or specific goals—can likely still find ways around these security measures.

Identifying high- and low-priority assets should guide internal cybersecurity planning and processes. Current protocols have many companies simply "chipping away" at the threats and slowly patching, but that approach can leave important systems exposed. Roundtable participants emphasized the importance of establishing priorities for protection—if a system has a million vulnerabilities, a company needs to decide what aspects of the system are most important and make sure those are properly protected. Companies may need to protect "crown jewels" and accept some level of vulnerability for the rest of their systems.

Information sharing about sector trends is crucial to identifying what needs to be protected—whether it is personally identifiable information, sensitive internal documents, username databases, network credentials, or access to industrial control systems (ICS). The Biden administration's ICS Cybersecurity Initiative is an example of how prioritizing can work. Recognizing the potential consequences that can stem from "the degradation, destruction, or malfunction of systems that control" critical infrastructure, there has been a concerted effort for the public and private sectors to work together to protect this type of infrastructure. So far, the administration has developed action plans for the electric, natural gas pipeline, and water sectors.

Companies may need to protect "crown jewels" and accept some level of vulnerability for the rest of their systems.

4. Create More Demand for Security

Roundtable participants agreed that MFA should be a standard, and then asked why it isn't the default for products and services. Some speakers asserted that it may be because there is no demand for MFA, meaning there is little incentive for most companies to use it.

The federal cybersecurity market for FY 2022 is somewhere between $14.4 billion and $20 billion. The Infrastructure Investment and Job Act, which became law in November 2021, includes close to $2 billion for cybersecurity. If passed, the Build Back Better Act would provide additional funding for cybersecurity programs. This federal market creates an opportunity to build incentives.

The May 2021 executive order already asks for a review of the Federal Acquisition Regulation (FAR) language to require enhanced security and reporting from information technology and operations technology service providers. During an earlier CSIS event, Anne Neuberger explained how the government can use its "power of procurement to set in place a standard and lift up the security of the software and tech that everybody is using." The General Services Administration, DOD, and NASA have proposed two amendments to the FAR. One would "increase the sharing of information about cyber threats and incident information between the Government and certain providers" and the other one would "standardize common cybersecurity contractual requirements across Federal agencies for unclassified information systems." According to the FAR Council, two Notices of Proposed Rulemaking will be issued for these amendments. The proposed rules will tackle two crucial issues: information sharing and common requirements. This latter item can be leveraged to increase cybersecurity for all.

CARROTS AND STICKS

5. Avoid a Confrontational Relationship

Finding the resources for proper cybersecurity is prohibitively costly for many organizations—contrary to public perception, even multinational corporations struggle with this. Some participants in the roundtables expressed concern that at times, the government is perceived as confrontational, fueling distrust between the public and private sectors. One executive noted that during the transition to work from home in the midst of the Covid-19 pandemic, their company received an FTC order detailing all the things the company was doing wrong. In another example, during the Log4j response, some companies received FTC warnings threatening legal action. This puts providers in the awkward position of having to ensure the compliance of third parties, straining their own relationship with their clients. However, relying only on voluntary actions is insufficient.

Implementing a response model akin to the Federal Emergency Management Agency's could help address this. This would provide victims with the people, money, and tools they need after a cyberattack. A focus on helping and supporting organizations could smooth the relationship between the public and private sectors and align their efforts and needs. The benefits from having the public and private sectors working side by side were demonstrated by the collaborative response to the Log4j vulnerability.

> *Some participants in the roundtables expressed concern that at times, the government is perceived as confrontational, fueling distrust between the public and private sectors.*

In late November 2021, a member of the Alibaba cloud security team discovered a security bug affecting Log4j, a popular piece of software that apps and services use to record user activity within an application.

The software flaw, called Log4shell, lets malicious actors use third-party servers to submit code on a targeted computer and allow them to remotely control the system. Once the exploit became public in early December, cybersecurity centers around the world rushed to inform potential targets—"a variety of consumer and enterprise services, websites, and applications"—about the vulnerability and advise them on how to identify and mitigate the threat. Given the wide array of Log4shell's potential uses, the burden of addressing the flaw fell mostly on the enterprise side.

In the United States, public-private collaboration in response to the threat has been characterized by a mix of requirements and information sharing. One of CISA's first actions was to convene the JCDC—an initiative that brings together government and private-sector representatives to coordinate cybersecurity planning and information sharing—and JCDC received favorable reviews from all participants. CISA offered a step-by-step guide for mitigation, detection rules, and a compilation of resources from JCDC partners, which included tools, analyses, and recommendations. Additionally, on January 4, 2022, the FTC issued a warning to companies to patch the vulnerability or risk legal action.

The government's response showcased how the different agencies can work together to respond to and mitigate a crisis. This collaborative approach and information sharing were described by CISA leaders as "unprecedented," and were highly praised by the private sector. This experience could serve as a charter of what collaboration can achieve for both sides.

6. Expand the Workforce

Participants agreed that there is a global shortage of cybersecurity professionals and that government action needs to be taken if this shortage is to be addressed. In the United States, some estimates suggest there are around 597,000 cybersecurity openings, while the existing workforce can only fill two-thirds of cybersecurity jobs. Another report by the International Information System Security Certification Consortium, or $(ISC)^2$, found that 377,000 cybersecurity professionals are needed to address the workforce gap. Whatever the shortfall, it is significant enough that the consequences from not having the appropriate staff are real: the $(ISC)^2$ report counts among them "misconfigured systems, slow patch cycles, rushed deployments, not enough time for proper risk assessment, not enough oversight of processes and procedures, and more."

Expanding the cybersecurity talent pool was a priority for the experts who participated in the roundtable series. There was broad support for promoting and expanding programs like the National Science Foundation's scholarship for service to enhance the workforce while providing much-needed talent to federal, state, local, and tribal governments. A cyber version of the Peace Corps could be shaped into a national push to increase the cybersecurity workforce. The program would entail the government paying for a four-year degree and in exchange, the student committing to five years of service. This would increase the ability for the cybersecurity field to recruit young people or even people in their mid-careers.

Diversity of the cyber workforce should be addressed in parallel. According to a report by the Aspen Institute, "only 4% of cyber - security workers self-identify as Hispanic, 9% as Black, and 24% as women." According to Camille Stewart, the global head of product security strategy at Google, lack of diversity in the workforce undermines efforts toward resilience, "limiting our ability to identify and address threats, innovate, and meaningfully cooperate with partners." Ensuring that efforts to develop cybersecurity talent target and include underrepresented communities is crucial for a robust workforce.

While some companies might be hesitant toward a CyberCorps program because of a reluctance to have federal employees working on their systems, there are mitigations. For example, the program could avoid this tension by placing individuals on higher-tier national critical functions handled by the private sector. Critical infrastructure entities are facing an acute workforce shortage, often having multiple openings for vital security positions.

Government-funded programs should be balanced with a concern for potential moral hazard; if companies become reliant on this stream of federally funded talent, they may lack the motivation to build their own cyber precautions. Successful workforce partnerships between the public and private sectors will take this into account.

> *Ensuring that efforts to develop cybersecurity talent target and include underrepresented communities is crucial for a robust workforce.*

7. Explore the Possible Role of Insurance Companies in Incentivizing Cyber Resilience

Participants liked the idea of using insurance to improve cybersecurity because it offers a nonregulatory mechanism that creates incentives, but insurance has not yet delivered. The U.S. Cyberspace Solarium Commission report, for example, recommends trying to shape the insurance market as a way to incentivize the implementation of better cybersecurity practices. Tying the expectation about coverage and risk to premiums and coverage might create a strong incentive.

There is already some precedent for the role of insurance companies in shaping the response to cyber incidents. In 2017, the NotPetya malware paralyzed business operations and caused billions of dollars in damage worldwide. Pharmaceutical company Merck estimated it had suffered $1.4 billion in damages. However, its insurers claimed that their coverage for loss or damage from the destruction or corruption of computer data and software would not apply in this case. Because the cyberattack was attributed to the Russian military, insurance companies stated the incident fell under the "hostile/warlike action exclusion." In December 2021, the Superior Court of New Jersey found the exclusion to be nonapplicable, and Merck was entitled to the coverage. This can encourage companies—at least those that can afford it—to self-insure.

Considering the fallout from the case, it is not surprising that insurance companies have made changes to policy terms. In November 2021, Lloyd's Market Association presented four exclusion clauses regarding cyber operations. Each offers a different level of coverage for cyber operations conducted during war, retaliatory cyber operations, or those that have a detrimental impact. The four clauses rely on governmental attribution for their application.

COOPERATION WITH INDUSTRY AND ALLIES

8. Build on the JCDC to Expand Cooperation among Companies

Like using insurance, information sharing is a traditional remedy to counter and mitigate cybersecurity risks. A new emphasis is on providing early warning of cyber incidents. Information-sharing programs allow the government to share information with the organizations that operate critical infrastructure. There are many existing programs, and Section 1550 of the FY 2022 NDAA requires the implementation of a pilot program with internet ecosystem companies "to discover and disrupt use by malicious cyber actors of the platforms, systems, services, and infrastructure of such companies." Sec. 1508 calls for the United States Cyber Command to establish a voluntary process through which it can engage with private-sector information technology and cybersecurity companies to defend against foreign malicious cyber actors.

In simple terms, these companies have insights—given the access their contractual status gives them to customer networks—that the government cannot obtain without a warrant. Private-sector cybersecurity firms will often spot malicious activity first; if there was a way, taking into account legal requirements, to aggregate and share this information, it would provide a much higher degree of awareness for all.

One of the challenges is determining who integrates this data and who should participate. Increasing the number of companies involved can boost capabilities and visibility, but to maintain effectiveness, the scope of action should be focused, and the number of participants limited. For starters, the priority could be to establish a program that includes more mature companies—for example, involving the providers of critical software as published by NIST.

Building on earlier work in establishing partnerships, CISA launched the JCDC in October 2021, which also provides operational planning and collaborative analysis. The successful use of the JCDC to face the Log4j vulnerability makes a good case for its continued use and expansion. It hopefully also signals a shift toward a more collaborative approach, one that sees the different responsible stakeholders working together. If companies decide not to share information about the threats they see and face, that can undermine the entire environment. Cementing trust between companies, as well as between the public and private sectors, will be essential.

Many of the recommendations on this topic require a strong commitment as much as resources. Companies can raise the floor for cybersecurity by sharing existing approaches and resources; engaging in information sharing is not limited to the relationship between the government and individual companies. Visibility on threats would benefit from cooperation across industries, among cybersecurity providers, and with DHS. Sharing concrete assets, like real-time dashboards, can help prevent and mitigate cyberattacks. The United Kingdom's National Cybersecurity Center, for example, successfully implemented a cyber threat intelligence information-sharing guide zserves as a way to partner with companies. While this approach may not be perfect, it shows how to get creative without having to sustain new funds.

> *Companies can raise the floor for cybersecurity by sharing existing approaches and resources; engaging in information sharing is not limited to the relationship between the government and individual companies.*

9. Expand Enforcement Cooperation with Allies

Cybersecurity is becoming a key part of the foreign policy agenda. To continue progress, participants believed that the United States, its allies, and partners should pursue the implementation of international norms for cyberspace to enhance accountability and responsible action. Supporting and promoting norms of responsible behavior and international law should be a priority, as well as raising the profile and stressing the urgency in diplomatic spheres.

Collaboration between national CERTs during an incident was found to be valuable by many of the participants from global companies, who drew on resources in more than their home country. A global company will have relationships with several national CERTs. Support and communication from more experienced CERTs can make a big difference for smaller company teams, who may be dealing with an overwhelming workload.

Another area participants believed would be useful to expanding collaboration is the arrest of bad actors. Some participants called attention to the FBI legal attachés in other countries. In a related vein, in October 2021, the United States convened the Counter Ransomware Initiative, which included representatives from 30 countries and the European Union to discuss the security threat posed by ransomware. One of the discussion points was, precisely, how to reinforce "timely and consistent collaboration across law enforcement, national security authorities, cybersecurity agencies, and financial intelligence units," recognizing the transnational nature of the threat to improving enforcement. ■

Eugenia Lostri *is an associate fellow with the Strategic Technologies Program at the Center for Strategic and International Studies (CSIS) in Washington, D.C.* ***James Andrew Lewis*** *is senior vice president and director of the CSIS Strategic Technologies Program.* ***Georgia Wood*** *is a program coordinator and research assistant with the CSIS Strategic Technologies Program.*

The authors would like to thank the public- and private-sector officials who participated in our roundtable series. The authors would also like to give special thanks to Andrew Braverman for his research assistance.

This report is made possible with support from HP Inc.

This report is produced by the Center for Strategic and International Studies (CSIS), a private, tax-exempt institution focusing on international public policy issues. Its research is nonpartisan and nonproprietary. CSIS does not take specific policy positions. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the author(s).