News Release

For more information:
Jonathan.Liu@tcb.org
Katie.Puello@tcb.org

CED Report: As Cyberattacks Intensify, Keeping the US Resilient Will Require Closer Public–Private Cooperation

New York, June 14, 2022…..Today, the Committee for Economic Development, the public policy center of The Conference Board (CED), issued a new Solutions Brief, ***Securing Cyberspace in an Era of Evolving Threats***. The report—the latest in a series on Sustaining Capitalism—illustrates the ever-growing threat of cyberattacks, especially ransomware attacks, and looks at the factors that make it harder to secure against such threats, including a talent gap. It also includes several recommendations for bolstering cyber protection and resilience and building a cyber workforce and talent pipeline.

The report's central theme is that leaders in the public and private sectors must work more closely together to better secure cyberspace. That will mean sharing information, collaborating against accelerating threats, and working in tandem to train a cybersecurity workforce large enough to protect Americans and their data. A cyberattack occurs in the United States every 39 seconds, a frequency that is only expected to increase, especially because the COVID-19 pandemic accelerated the use of cloud services and other digital technologies.

"Cybersecurity is no longer just an issue for the IT department, but is now a critical responsibility for CEOs, c-suites, and boards in all organizations," said **Dr. Lori Esposito Murray, President of CED**. "This responsibility won't be met effectively without more robust coordination and partnerships between public- and private-sector leaders—spanning major corporations to smaller businesses to the federal government to state and local governments. Cyber threats are growing in numbers, complexity, and intelligence, underscoring the importance and urgency of acting against cyber criminals while also making our systems significantly more resilient."

Key insights from the Solutions Brief include:

Cyberattacks are increasing in frequency and seriousness

- A cyberattack occurs in the US every 39 seconds.
- Ransomware poses a particular threat, having been used in 60 percent of malware attacks on companies in 2021—up from 45 percent in 2020.
- 76 percent of companies report having been victimized by ransomware.
- In 2021, 90 percent of ransomware attacks on businesses impacted their ability to operate.
- In 2021, in 68 percent of attacks, cybercriminals distributed ransomware by email or social engineering (e.g., phishing, baiting, scareware).
- Experts predict that, by 2031, ransomware will cost $265 billion globally, up from $20 billion in 2021.

Cybercriminals are varying their targets and methods

- Attacks on large organizations are usually targeted, with a goal of stealing sensitive data and potentially demanding a payment.
- While attackers have traditionally used a random, "spray-and-pray" approach to attack smaller companies, they are increasingly targeting those businesses as data becomes more valuable.
- In 2021, 74 percent of all cyberattacks were targeted, up from 70 percent in 2020.
- According to one estimate, 74 percent of all money made through ransomware attacks went to Russian hackers.
- Cybercriminals have also started targeting supply chains to maximize the impact they have on organizations that they attack.

- The three most frequently attacked sectors in 2021 were government (16 percent), healthcare (11 percent), and manufacturing/industry (10 percent).

The US faces a cybersecurity workforce deficit

- 88 percent of businesses hit by ransomware report that they have an insufficient cybersecurity budget, with the same percentage saying that they don't have enough cybersecurity workers.
- The US added more than 260,000 cybersecurity jobs in 2021, a 30 percent increase. But as of early May 2022, there were 600,000 vacant US jobs in the sector.
- On average, 50 percent of hiring managers believe that applicants are not well-qualified, which helps explain why it takes six months to fill a new cybersecurity position.

Key recommendations from the Solutions Brief include:

In its Solutions Brief, CED makes several recommendations for public/private collaboration to improve cyber protection and resilience, broken into seven sub-recommendations, and on building a robust cybersecurity talent pipeline:

- **Strengthen cyber protection and resilience**. This recommendation has seven components:

    1. **Government and private-sector leaders should collaborate and share information.** The federal government should enhance collaboration and information-sharing with other levels of domestic government, the private sector, and internationally to combat and protect against threats. Cybersecurity is not limited by borders or boundaries. Businesses should document cyber incidents and threats and proactively communicate with their supply chains, customers, and other stakeholders in a timely manner to maintain their reputations and to protect all parties involved. The Cybersecurity and Infrastructure Security Agency (CISA) should promote, strengthen, and incentivize active participation in current information-sharing efforts such as Information Sharing and Analysis Organizations, the Cyber Information Sharing and Collaboration Program, and the Enhanced Cybersecurity Services program.

    2. **CISA should expeditiously implement the March 2022 Cyber Incident Reporting for Critical Infrastructure Act.** It should take the lead and expedite the implementation of cyber reporting requirements and remove information-sharing barriers, possibly including through legislation. CISA should coordinate across the federal government to provide clear guidance to public- and private-sector organizations on how to report cyber incidents and reduce the reporting burden for organizations by sharing information across Federal government agencies. It should compile and regularly publish the information.

    3. **The federal government should expand resources available to small- and medium-sized organizations.** Under the National Cyber Director's leadership, it should continue programs like CISA's cyber hygiene service to critical infrastructure organizations while expanding the resources available to other organizations. Government and private-sector leaders should collaborate to expand the free resources available to small- and medium-sized organizations to build cyber resiliency and increase protection. Protecting these businesses is critical to protecting critical infrastructure supply chains. The government, in collaboration with the private sector through an entity like the Cybersecurity Advisory Committee, should create streamlined action and implementation guidance and resources to aid small- and medium-sized businesses with limited resources. Highlighting and broadly communicating the most critical points and actions will aid in building protection quickly.

4. **Public- and private-sector leaders should develop, validate, monitor, and promote effective standards.** They should work together to continue to develop, validate, and promote best practices for cybersecurity through committees, "sprints," or other collaborative arrangements. As technology advances, so do the cybercriminals' methods. Standards for newer technologies, such as artificial intelligence, should be developed and monitored for compliance where needed to protect critical infrastructure or public safety. Clear guidance should be provided so that standards are consistently applied. Additionally, proactively sharing across organizations and sectors will help organizations and individuals prevent costly attacks. Too often, methods that could have prevented devasting attacks are only shared afterward.

5. **The federal government should provide a unified cybersecurity approach.** Compiling resources for the private sector from across the government in one location and providing clear messaging is critical. CISA should lead the development of a one-stop shop of cybersecurity resources and information to eliminate confusion and aid with implementation.

6. **Public- and private-sector leaders should build organizational resilience by implementing fundamental cyber protection for their most valuable and vulnerable assets, as well as building cyber resiliency in case of a successful attack.** Employee training should be frequent, and content should be updated regularly to reflect changing conditions and threats. Working toward a Zero-Trust Architecture security model and implementing recommended software patches and updates should be ordinary course. Organizations should identify and work to mitigate supply chain vulnerabilities. Working across organizations will strengthen cyber protection. Organizations should take advantage of all available federal resources.

7. **Business and governmental leaders should champion partnerships and develop and collect success metrics to track how they do.** Business leaders should form partnerships within economic sectors and in coordination with CISA to leverage comparative advantages and to share resources, where appropriate. Ideally, success metrics should be collected and reported to CISA to promote replication and scaling of successful partnerships.

- **Build a robust cyber workforce and talent pipeline**:

1. **Public- and private-sector leaders should devote more resources to the cyber workforce to attract and maintain a robust, diverse, and highly skilled talent pool.** Cybersecurity education programs should provide the skills and knowledge for graduates to enter the field with immediately applicable skills. Strive to attract new and diverse talent to the cybersecurity workforce. Provide incentives and transition paths for workers to enter and remain in the cybersecurity workforce. Develop new apprenticeships, bootcamps, workforce accelerator programs, or other training vehicles to skill, upskill, and reskill workers for cyber careers. The federal government should expedite the cyber professionals' hiring process. It should also consider opportunities for private employees to contract or detail with the federal government to leverage talent across sectors. Where possible, scholarships should be extended to help make cybersecurity education more accessible to a diverse set of candidates.

2. **The federal government should create a virtual national academy for cybersecurity.** Separate from the military but following the current model of military service academies, cadets in the cybersecurity national academy would receive a free college education in return for five years of government cybersecurity service upon graduation. Cybersecurity courses would be the main focus of the education with partnering colleges and universities providing supplemental coursework. Graduates would be placed in federal, state, or local government cybersecurity roles upon graduation.

The new Solutions Brief, ***Securing Cyberspace in an Era of Evolving Threats***, can be accessed here.

Media Contacts
Jonathan.Liu@tcb.org
Katie.Puello@tcb.org

About CED
The Committee for Economic Development (CED) is the public policy center of The Conference Board. The nonprofit, nonpartisan, business-led organization delivers well-researched analysis and reasoned solutions in the nation's interest. CED Trustees are chief executive officers and key executives of leading US companies who bring their unique experience to address today's pressing policy issues. Collectively they represent 30+ industries, over a trillion dollars in revenue, and over 4 million employees. www.ced.org

About The Conference Board
The Conference Board is the member-driven think tank that delivers trusted insights for what's ahead. Founded in 1916, we are a non-partisan, not-for-profit entity holding 501 (c) (3) tax-exempt status in the United States.
www.conference-board.org