Energy & Manufacturing Competitiveness Partnership

Secure.

Ensuring Resilience & Prosperity in a Digital Economy

Compete.

Council on Competitiveness

Executive Summary

The interconnectedness and openness made possible by the Internet and the broader digital ecosystem create unparalleled value for society. The architects of the Internet could not know, however, that it would reach the breadth and scope seen today.

In 2018, the U.S. Department of Homeland Security (DHS) declared that cyber weapons and sophisticated hacking pose a greater threat to the United States than the risk of physical attacks. With the U.S. economy losing between $57 billion and $109 billion per year to malicious cyber activity,[1] it is clear that in order to remain secure and competitive, the United States needs a comprehensive national policy agenda in the cybersecurity space.

In recognition of the growing importance of cybersecurity to America's economic and national security, the Council on Competitiveness in 2018 launched a three-dialogue series on increasing the resilience of the nation's critical infrastructure, intellectual property and industrial operations against cyber-attack. The series, co-chaired by Dr. Steven Ashby, director of Pacific Northwest National Laboratory, Mr. George Fischer, senior vice president and group president of Verizon Enterprise Solutions, and Dr. Farnam Jahanian, president of Carnegie Mellon University, focused on the security and economic challenges posed by the increasing cyber threat and sought to identify mechanisms for building resilience in the new battlefield of digital warfare.

The cybersecurity initiative engaged more than 150 experts and consisted of three dialogues, each of which sought to identify the challenges and opportunities in distinct sectors of the economy. The first dialogue, hosted by Verizon in New Jersey in February 2018, examined the role of the private sector in U.S. critical infrastructure. The discussion made clear that despite the clear importance of cybersecurity in the current technological and political climate—and the threat cyber-attacks pose to critical infrastructure and intellectual property, and therefore to business operations and national security—resource constraints, both financial and human, are pervasive.

At the second dialogue, hosted by Pacific Northwest National Laboratory in Seattle in April 2018, experts across multiple sectors gathered to assess and make recommendations on the state of cybersecurity as it relates to U.S. national security. The conversation called attention to the lack of coordination across various sectors and agencies, the need to incentivize best practices in security and the importance of leveraging local and regional assets to prepare and respond to cyber-attacks.

The third and final dialogue in the series, hosted by Carnegie Mellon University in Washington, D.C., in June 2018, sought to engage federal policymakers from Capitol Hill and the administration in this important conversation and to develop an actionable agenda to improve U.S. resilience to cyber threats.

1 *The Cost of Malicious Cyber Activity to the U.S. Economy*, The Council of Economic Advisors, February 2018.

Together, the challenges, opportunities and recom-mendations discussed throughout the three cybersecurity dialogues—and throughout the EMCP's six sector dialogues—formed the foundation for the Council's National Agenda for Cybersecurity presented in this report.

The cybersecurity work was conducted under the umbrella of the Council's Energy and Manufacturing Competitiveness Partnership (EMCP), a C-suite-directed initiative focused on the shifting global energy and manufacturing landscape and how energy transformation and demand are shaping industries essential to America's prosperity and security. Critically, the EMCP approached America's diverse industrial landscape not as a monolith but as a network of distinct but interdependent productive sectors, each with its own challenges and opportunities. Throughout the exploration of six critical sectors of the U.S. economy, it became clear that cybersecurity is a significant issue that cuts across all industries and sectors, and that the United States is in need of a coordinated strategy for addressing this growing challenge.

The genesis of Council's work in this space, however, dates back to long before the launch of the EMCP in 2015. Released in 2007, Transform. The Resilient Economy: Integrating Competitiveness and Security declared, "The challenge is not security; it is resilience." The report promoted a strategy of resilience for both the public and private sectors—one that called for building America's capability to survive, adapt, evolve and grow in the face of challenges. While the challenges may have changed in the last ten years, the link between competitiveness and security is stronger than ever.

The National Agenda for Cybersecurity has the power to secure and strengthen America's resilience to the growing cyber threat while ensuring America remains a competitive, productive and prosperous nation.

A National Agenda for Cybersecurity

A national cyber agenda must ensure the United States has the infrastructure, technology and talent needed to build resilience to cyber-attacks, along with the ability to respond and recover in the event of such attacks.

The interconnectedness and openness made possible by the Internet and the broader digital ecosystem create unparalleled value for society. The architects of the Internet could not know, however, that it would reach the breadth and scope seen today. Throughout human history, technological advancement has outpaced security. While this is unlikely to change, America's ability to remain resilient in the face of increasing cyber threats will require a shift in the understanding of—and dynamic between—innovation and security. The evolution to a new way of thinking that focuses on deliberate, risk-informed trade-offs will be essential.

What follows are a series of concrete, actionable recommendations cutting across the public and private sectors that, taken together, will strengthen U.S. cyber defenses and ensure greater resilience in the face of growing and malicious cyber threats.

Secure America's Critical Assets and Infrastructure Against Cyber-attacks

With the average cost of a data breach in the United States at an all-time high of $7.91 million and over 1,300 significant breaches in the last year, malicious cyber activity in the United States is a substantial threat to America's economic and national security.[32] The increasing sophistication of cyber-attacks poses a constant threat to critical infrastructure. And as the availability of networks is called into question every day, the economic viability of U.S. businesses and the freedoms Americans exercise daily are in jeopardy.

1. Curtail the foreign acquisition by hostile actors of American cybersecurity assets to better manage risk. Regional powers have a growing potential to use purchased cyber tools to conduct catastrophic attacks on U.S. critical infrastructure.[33] While cyber threats from state and non-state actors come in many forms, including cyber-crime and military and political espionage, the acquisition by hostile foreign governments of U.S. cyber assets constitutes a significant security risk for the United States.

Recommendations

1.1. Require under the new authorities of the Foreign Investment Risk Review Modernization Act (FIRRMA) in the National Defense Authorization Act for Fiscal Year 2019 that the Committee on Foreign Investment in the United States (CFIUS) conduct full reviews and regulatory approval for any foreign investment or ownership interest in American advanced cybersecurity startups, joint ventures or acquisitions.

32 *2018 Cost of a Data Breach Study*, Ponemon Institute, July 2018.

33 *Task Force on Cyber Deterrence*, Department of Defense Defense Science Board, February 2017.

1.2. Require all U.S. securities and SEC-registered securities and investment funds of any size to provide the U.S. Department of the Treasury and the FBI full transparency on sources of investment capital and intellectual property, and limit partners from countries deemed high-risk or sanctioned by the Treasury Department.

1.3. Expand the authority of the Bayh-Dole Act and federal tech transfer act to prevent the licensing of U.S. cyber technology developed with federal funding to foreign countries deemed high risk.

2. Leverage public and private sector purchasing power to ensure cybersecurity protections are upfront requirements throughout the value chain. While DoD contractors and subcontractors are required to meet certain security protocols, there is no universal clause across federal procurement contracts. And, industry largely lacks a consistent approach to applying best practices for security design, development and deployment of Internet-connected devices.

Recommendations

2.1. Extend Defense Federal Acquisition Regulation Supplement DFAR 252.204-7012 language mandating adequate security to all government agencies.

2.2. Call on Congress to take immediate action on the Internet of Things ('IoT') Cybersecurity Improvement Act of 2017, requiring the inclusion of specific cybersecurity protections in procurement contracts with all federal and state agencies for Internet-connected devices.

2.3. Incentivize vendors' awareness and adoption of security best practices utilizing industry purchasing power.

2.4. Promote greater uptake and use of existing cybersecurity standards to increase supply chain security.

3. Establish a means of coordinating cyber R&D investments and research agendas. When it comes to cybersecurity research, there is no community-defined research agenda, resulting in duplication of efforts and inefficient use of limited financial and human resources.

Recommendations

3.1. Establish the National Cybersecurity R&D Initiative, chaired by the White House Science Advisor, to identify challenges, solicit industry input, define priorities and, on an ongoing basis, coordinate government investment to optimize talent and resources and avoid duplication of efforts.

3.2. Convene a Basic Research Needs working group including leaders from the public and private sectors to define a set of research priorities to address the technology R&D challenges and Science Grand Challenges that, if solved, will strengthen U.S. cybersecurity capability.

3.3. Create data-driven processes to develop specific cybersecurity countermeasures unique to sectors and sub-sectors, and disseminate these processes through Information Sharing and Analysis Centers and Community Emergency Response Teams to mitigate the risk of cyber incidents.

4. Develop, upgrade and deploy cybersecurity technology to enhance America's resilience to cyber-attacks. The pace of technological advancement is accelerating at record speeds, increasing vulnerability to data theft and operational disruption increases. As the threat of cyber-attacks becomes more grave, products and processes must be designed to meet basic security standards.

Recommendations

4.1. Require that all new technology applied to the electric grid meet industry standards to ensure basic cybersecurity.

4.2. Expand funding and private sector engagement for testbeds for the creation and adoption of new cybersecurity technologies such as Digital Manufacturing Design and Innovation Institute (DMDII) Cyber Hub for Manufacturing and the Army Cyber-research Analytics Laboratory.

4.3. Expand the NIST cybersecurity framework to better guide secure development of IoT, operational technology (OT) and information technology (IT) platforms and technologies as a means to bolster private industry certification programs.

Strengthen America's Cyber Response and Recovery Capabilities

According to the latest data, in the United States, the average time required to identify a data breach incident is 201 days, while the average amount of time to contain a breach is 52 days.[34] America's ability to detect, withstand and recover from cyber events that disrupt the economy and society in a quick and coordinated manner is essential for the nation's security and competitiveness.[35]

5. Enhance coordination across departments and agencies at the federal and state levels responsible, with the goal to improve resiliency and response to cyber threats. While numerous federal agencies are factoring cybersecurity into their programming and funding, there is minimal coordination across departments.

Recommendations

5.1. The administration should reinstate and empower a White House cybersecurity czar to oversee a government-wide interagency task force to develop and implement, within 180 days, a coordinated cyber defense strategy that includes mechanisms for owners and operators of critical infrastructure to more easily share appropriate data.

5.2. Governors should convene state and local representatives from across the public and private sectors to develop statewide cyber-attack prevention and response strategies.

34 "IBM Study: Hidden Costs of Data Breaches Increase Expenses for Businesses," PRNewswire, IBM Security, July 11, 2018.

35 "Protecting Small Businesses from Cyber Attacks: the Cybersecurity Insurance Option", Testimony of Robert Luft, Owner, Surefire Innovations, National Small Business Association, July 26, 2017.

5.3. Convene biannual meetings of the private sector chairpersons of federal government advisory committees and external boards to share agency priorities, best practices and identify areas to strengthen interagency collaboration.

6. Develop agile, mobile and technically trained state and/or regional coalitions of cyber first-responders. Current recovery times from cyber-attacks are long and protracted, threatening American security and economic interests. With the average cost of a data breach in the United States at an all-time high of $7.91 million,[36] efficient incident response is critical and current assets are insufficient.

Recommendations

6.1. Institute state Cyber Protection Teams through the National Guard Bureaus and tactical analysis groups.

6.2. Governors and state legislators must provide funding and reduce legal and liability barriers to resources acting in state capacity.

6.3. Expand to additional states existing programs[37] to provide veterans with access to cybersecurity training opportunities and resources to help veterans enter the cybersecurity workforce.

6.4. Establish and fund, at the state level, "civilian reserve cyber corps" comprising volunteers from private industry security and IT professionals to be deployed in the event of a regional cyber incident.

6.5. Create a tiered technology approach to cyber that enables technically-trained cyber experts—people who are experts in using tools but that don't require advanced degrees—to obtain the technical skills needed to act in this capacity.

7. Expand access to cyber resources for small and medium-sized companies. Small businesses—those with fewer than 100 workers—represent more than 98 percent of total businesses in the United States.[38] In fact, 58 percent of data breach victims are small businesses.[39] Small businesses estimated their average cost for incidents in the last 12 months to be $34,604.[40]

Recommendations

7.1. Sustain funding for the Manufacturing Extension Partnership (MEP) National Network and expand resources available for cybersecurity tools and training and certification such as the NIST MEP Cybersecurity Assessment Tool.

7.2. State and metropolitan Small Business Administrations should establish cybersecurity training initiatives in partnership with Workforce Development Boards to reach a broad array of small and medium-sized businesses below the cyber poverty line.

7.3 Expand federal and state outreach to small and medium-sized businesses to increase knowledge of existing resources, including top resources identified by the DHS U.S. Computer Emergency Readiness Team (US-CERT).

36 *2018 Cost of a Data Breach Study: Global Overview*, Ponemon Institute, July 2018.

37 Cyber Virginia: Cyber Veterans Initiative, The Commonwealth of Virginia, July 2017.

38 *Annual Survey of Entrepreneurs*, U.S. Census Bureau, 2016.

39 *2018 Data Breach Investigations Report*, Verizon, 2018.

40 *2018 HISCOX Small Business Cyber Risk Report,* Hiscox Inc, 2018.

8. Engage corporate leadership in the development of procedures necessary to plan for, respond to and recover from cyber incidents. Cybersecurity has become an urgent concern for companies of all sizes and across all industries. Cyber threats pose significant risks to economic security and competitiveness and have become increasingly costly in terms of detection and response.

Recommendations

8.1. Corporate cybersecurity leads should report directly to executive team members and align responsibilities with risk management strategies.

8.2. Companies should embrace the Securities and Exchange Commission Guidance on Public Company Cybersecurity Disclosures[41] and take all required actions to inform investors of material cyber risks and incidents in a timely fashion.

Develop and Deploy a 21st Century Cyber Workforce

Further adding to the growing risk of cyber threats to American prosperity, the world is on pace to reach a cybersecurity workforce gap of 1.8 million by 2022.[42] It is vitally important that the United States have an adequate cybersecurity workforce to secure the nation's critical infrastructure; respond to the ever-expanding cyber threat; and equip businesses of all sizes and governments at all levels with the talent to meet the next generation of cyber challenges.

9. Expand and upskill the cybersecurity workforce to meet the complex and growing cyber threat. The cybersecurity field faces a constant shortage of practitioners, with approximately 350,000 current cybersecurity openings unfilled, according to CyberSeek, a project supported by the National Initiative for Cybersecurity Education (NICE).

Recommendations

9.1. Ensure NSF funding for the CyberCorps®: Scholarship for Service (SFS) program meets the growing demand.

9.2. The National Science Foundation should expand and expedite the implementation of the Community College Cyber Pilot Program (C3P) under the CyberCorps® SFS program.

9.3. Congress should take immediate action to pass S. 754, Cyber Scholarship Opportunities Act of 2017 to permanently extend support for cybersecurity education in primary and secondary schools.

9.4 Expand cybersecurity awareness programs in secondary schools to increase interest and awareness of students from diverse backgrounds regarding career opportunities in the cybersecurity field.

41 Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 2018.

42 *2017 Global Information Security Workforce Study*, Frost & Sullivan, 2017.

10. Reform curricula at the nation's colleges and universities to better meet the demand for cyber-savvy students and workers. The race to respond to cyber workforce needs has led to inconsistency in program quality and stove piping of expertise. The ability of academia, industry and government to address these challenges while meeting the growing workforce demand will be a key driver of American competitiveness.

Recommendations

10.1. Expand the number of colleges and universities with programs and credentials that meet the criteria required for designation as National Centers of Academic Excellence in Cyber Operations or Cyber Defense by the National Security Agency and the DHS.

10.2. Embed cybersecurity concepts into a broad range of existing degree programs at the university level.

11. Break down legal and organizational barriers prohibiting or limiting cybersecurity practitioners from serving as educators. While there are significant challenges around a mismatch between supply and demand of cybersecurity professionals, academia faces a compounding challenges of a lack of educators to train the workforce of tomorrow.

Recommendations

11.1. States and educational institutions must reduce barriers to allow cybersecurity practitioners to serve as professors of practice.

11.2. Establish industry-academia-national laboratory exchange programs to facilitate cross-pollination between cyber experts and practitioners.

Boost Cyber Awareness Among Policymakers and the Public

Human error is one of the most significant challenges when it comes to protecting against cyber-attacks. In fact, 90 percent of cyber incidents are human-enabled,[43] while as many as 24 percent of attacks may be due to employee actions or mistakes. [44]

12. Increase the awareness and understanding of cybersecurity issues among members of Congress and their staffers. With at least 36 states, D.C. and Puerto Rico having introduced and/or considered more than 265 bills or resolutions related to cybersecurity[45] and as many as 12 committees holding jurisdiction over various departments, agencies and programs addressing cyber issues, all policymakers on Capitol Hill must understand the technology and implications of cyber threats.

Recommendation

12.1. Members in the House of Representatives and Senate should reinvigorate the bipartisan House and Senate Cyber Caucuses, which have been largely dormant in recent years, to provide members of Congress and their staffers with access to experts in the field.

43 Shifting the Human Factors Paradigm in Cybersecurity, Calvin Nobles, Ph.D., March 15, 2018.

44 2016 Data Security Incident Response Report, BakerHostetler, 2016.

45 Cybersecurity Legislation 2018, National Conference of State Legislatures, May 18, 2018.

13. Increase the cyber awareness of the general public. An ever-evolving number of cyber threats target what is, in many ways, the weak link in the U.S. cyber ecosystem—the general public. Spam, phishing, spyware, malware, trojan horses and a litany of targeted consumer attacks can ruin personal financial security and be a gateway to a broader attack with the consumer as the entry point. Cyber savviness is no longer a luxury, but a necessity for all Americans.

Recommendations

13.1. Fund, develop and implement a major national cyber-awareness campaign, that builds on existing efforts, to increase the general public's awareness and capability to prepare for and respond to cyber threats.

13.2. Call on local economic development authorities to put in place programs that encourage cybersecurity education at the K-12 level.

13.3. Implement and enforce basic cybersecurity protocols throughout industry, government and academia including patching, multi-factor authentication and identity management as standard business practices.

"With the proliferation of interconnected devices, industries and organizations, the need for cyber expertise is quickly outpacing supply, creating an urgent need for colleges and universities to innovate curricula and program offerings in this field."

Dr. Farnam Jahanian
President
Carnegie Mellon University:

Council on Competitiveness
900 17th Street, NW, Suite 700, Washington, D.C. 20006, T 202 682 4292
Compete.org

@CompeteNow
facebook.com/USCouncilonCompetitiveness
linkedin.com/company/council-on-competitiveness/