U.S. CHAMBER OF COMMERCE

National Security and Emergency Preparedness Department
2017 Cybersecurity Policy Priorities (Select Examples)

The U.S. Chamber of Commerce has made economic growth its driving focus for 2017. Recent years have seen a surge of business and government investments and innovations in the field of cybersecurity. Policy developments used to be driven almost exclusively by government, but today companies are valuable partners in the quest to protect U.S. networks and information systems.

Enhancements to America's information security will help drive growth in our economy. Through sharing ideas, innovations, and visions with one another, business and government leaders are better able to coordinate efforts and anticipate challenges that could impact organizations' security and resilience. Some key policies that the Chamber seeks to advance this year are as follows:

Advocating for the Cybersecurity Framework and Supporting Small Businesses

The Chamber urges the administration to support the flexible industry-National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* (the Framework). The voluntary Framework, which the Chamber actively promotes through its national campaign, has received much praise from public and private organizations at home and overseas.

Small and midsize businesses (SMBs), which account for a significant percentage of all U.S. businesses, are more innovative, agile, and productive than ever, owing to the capabilities delivered by information technology (IT). To be sure, since IT is critical to the delivery of goods and services for all businesses, smartly addressing risks associated with doing business in a cyber environment must be a priority. State and local governments should also make cyber a priority.

- The White House and agency chiefs need to work with regulated industry sectors to harmonize cyber regulations with the Framework. The Chamber wants to see this initiative begin this year. Streamlining overlapping and/or conflicting cyber red tape is a top priority.

- The development and use of cyber metrics is a work in progress. Businesses regularly use quantitative and qualitative data to understand the status of their organizations' information security programs. Yet such subjective data are held closely by these businesses. Industry actors should never be compelled formally or informally to disclose metrics to third parties.

- The federal government should support ambitious public- and private-sector efforts to help private enterprises manage cyber supply chain risks internally and with their suppliers and partners. Examples include NIST's January 2017 draft update to the Framework, in which the Chamber is a participant.

- Government and business leaders should consider ways to help SMBs and state and local governments use the Framework and analogous tools (e.g., NIST's *Small Business Information Security: The Fundamentals* guide).

Leveraging Cyber Threat Information and Incident Data

Most policy and business observers agree that effective cyber information sharing is an important method of protecting organizations' computer systems. The Cybersecurity Information Sharing Act of 2015 (CISA) is off to a good start and does not need amending.

In addition, the Chamber commends the Commission on Enhancing National Cybersecurity's (the Commission's) push to create "reverse Miranda protections" for industry. Businesses should be able to freely discuss cyberattacks in a safe venue without fearing that regulators would use the information against them with respect to liability, rulemakings, and public disclosure.

Further, the Chamber endorses piloting a CIDAR—shorthand for a cyber incident data and analysis repository. An experimental CIDAR, initially administered by the Department of Homeland Security (DHS), can offer tangible upsides to U.S. cybersecurity, including helping insurers develop cyber coverage and best practices for their customers.

- To establish so-called reverse Miranda protections, the administration and Congress should work with industry to identify changes in statutes, regulations, or policies urging companies to voluntarily share information about their risk management practices.

- Private and government entities should join the Chamber in urging businesses to use the Framework, become a member of an information-sharing body, and take advantage of the CISA/Automated Information System (AIS) as appropriate.

- Data submitted to a CIDAR need to be made anonymous, and additional sharing protections would probably be needed.

Protecting the Internet of Things (IoT) and Increasing Businesses' Gains

Many companies go to extraordinary lengths to incorporate security into the design phase of the IoT devices that they make and sell globally. The Chamber wants both device makers and buyers to gain from the business community leading the development of state-of-the-art IoT components that can be used in settings such as manufacturing, transportation, energy, and health care. Strong IoT security should be a win-win proposition for both makers and purchasers.

- The Department of Commerce, especially NIST, did an admirable job convening many organizations to develop the Framework. The Chamber believes that the department is well-positioned to convene IoT stakeholders to identify existing standards and guidance.

Embedding Cybersecurity in Global, Industry-Driven Standards and Fixing Wassenaar

Cybersecurity standards and best practices are optimally led by the private sector and adopted on a voluntary basis. They are most effective when developed and recognized globally. Such an approach would avoid burdening multinational enterprises with the requirements of multiple, and often conflicting, jurisdictions.

Also in the international realm, "intrusion software" provisions were added in 2013 to the Wassenaar Arrangement's (WA's) list of dual-use goods and technologies subject to export control. The language used by the WA has unintended consequences that undermine defensive cybersecurity.

- International policymakers should align their cyber programs with the Framework, which is biased toward a standards- and technology-neutral approach to managing cyber risks.

- Policymakers need to support NIST's strategic engagement in international standardization to attain U.S. cyber objectives.

- The Chamber will press the administration to engage in the 2017 WA negotiations to achieve meaningful changes to the controls on intrusion software. The administration should refrain from implementing the controls on intrusion software until the core defects in the WA are fixed.

Clarifying Federal and Industry Roles and Responsibilities and Getting Government Resources Right

It is constructive that the Commission called for continued work on clarifying the roles and responsibilities of the public and private sectors. On paper, the Department of Justice (DOJ) and the FBI investigate and prosecute cybercrimes. DHS leads the protection of critical infrastructure. The Department of Defense (DoD) defends the nation from major attacks that are synonymous with acts of war. It's not clear to the Chamber that the three groupings have the resources and the interagency coordination they need to excel in the duties policymakers assigned to them.

Relatedly, federal agencies should lead by example on improving U.S. cybersecurity. In the last Congress, the Chamber supported the Modernizing Government Technology Act of 2016 (MGT Act). Many parts of the federal government's IT infrastructure are woefully outdated. The MGT Act authorized two IT modernization funding streams to improve, retire, or replace current technology systems and much more.

- Many companies tell us that they remain uncertain when their obligations to guard their enterprises from a cyber incident end—particularly in the wake of a nation-state attack—and the government's assistance begins. The process for handing off the cyber baton warrants deeper discussion, comprehension, and exercise.

- Future congressional legislation and the fiscal 2018 budget process give stakeholders the opportunity to better sync missions of the DOJ/FBI, DHS, and the DoD with the resources allotted to them.

- The Chamber intends to support legislation similar to the MGT Act in the 115th Congress.

Writing a New Cybersecurity Strategy That Features Business Input and Negotiating Toward Acceptable Behaviors in Cyberspace

Despite the existence of written doctrines (e.g., defense and international strategies), the U.S. cybersecurity strategy is seemingly uncertain both to many in the private sector and our adversaries. America's approach to cyber is at an inflection point. Industry is frequently the first to bear the brunt of cyberattacks coming from our nation's adversaries, and public policy should be adjusted accordingly.

- Policymakers should discuss the United States' cyber strategy with the business community before, during, and after the strategy is written. A wide range of issues must be wrestled with among multiple government and industry parties. In the cyber arena, authorities' intentions are often not accomplished without the significant buy-in of many sectors and companies.

- The Chamber supports commerce, not conflict. Defense and resilience must be the strategy's core pillars. Indeed, a strategic priority should be to increasingly deny our opponents' ability to conduct harmful cyber activity against the business community and the nation.

- Public-private policymaking needs to spotlight increasing adherence to international norms and deterrence. U.S. deterrence policy has so far prevented cyberattacks that may cross the line into armed conflict. But our national deterrence deficit lies in our struggle to stymie attacks by criminal groups and foreign powers that fall into the malicious middle of the attack spectrum. This middling sweep of aggressions is bookended on the one hand by relatively minor attacks (e.g., pings) and acts of war on the other.

(Revised March 2017)