

Securing Cyber Resiliency

BY 2021, GLOBAL
COST OF
CYBERSECURITY
WILL REACH

\$6
TRILLION
PER YEAR

The relentless pace of cyberattacks underscores the need for industry and government to work together to share information and establish effective cyber risk management approaches; neither government nor private-sector alone can effectively combat these threats. Cyber threats are best managed through a public/private partnership, and USTelecom is a dedicated partner.

USTelecom and its members work closely with numerous government and industry stakeholders in a broad variety of cyber infrastructure resilience initiatives.

- Our partnerships within DHS's Cybersecurity and Infrastructure Security Agency (CISA) and the DHS National Risk Management Center are designed to promote greater coordination and collaboration across critical infrastructure sectors and increase education and awareness efforts related to cybersecurity threats, information sharing, and incident response.
- Our collaboration with the National Telecommunications and Information Administration (NTIA) and the National Institute of Standards and Technology (NIST) under the Department of Commerce have helped develop practical frameworks for companies of all sizes to ensure their systems and processes are as secure as possible and are current with industry best practices.

EXAMINING SUPPLY CHAIN THREATS

USTelecom supports, and our sector seeks to work with, an ongoing federal risk management effort to identify IT and communications supply chain risks and devise appropriate remedial measures. USTelecom is proud to co-chair the DHS's new ICT Supply Chain Risk Management Task Force.

Given the complexities and overlapping interests of the communications supply chain, the federal government should evaluate and act upon supply chain threats using a consistent "whole of government" risk management methodology, strongly informed by the intelligence and trade communities, and other entities with the insights and capabilities to make well-informed supply chain risk determinations on behalf of the nation. The ICT Supply Chain Risk Management Task Force plays a key role in this mission.

Cyber threats are best managed through a public/private partnership, and USTelecom is a dedicated partner.

BY 2023
50%

OF ALL GLOBAL
DATA BREACHES
WILL OCCUR IN
THE U.S.

CSDE/ANTI-BOTNET EFFORTS

To demonstrate the importance of industry leadership, USTelecom, alongside the Consumer Technology Association (CTA) coordinates the **Council to Secure the Digital Economy (CSDE)**. CSDE and its members advocate for a globally harmonized policy environment that encourages innovation and investments in ever-advancing levels of security.

CSDE develops the **International Botnet and IoT Security Guide**. The guide, updated annually, encourages collective and responsible action throughout diverse segments of the internet and communications ecosystem, tackling the problem of botnets from many angles.

Specifically, the Guide addresses five segments: (1) Infrastructure, (2) Software Development, (3) Devices and Device Systems, (4) Home and Small Business Systems Installation, and (5) Enterprises.

The U.S. government has fully embraced this effort via NTIA's Botnet Roadmap, which incorporates CSDE's efforts into its own efforts to combat botnets. The U.N. Internet Governance Forum has recognized the CSDE guide among the world's leading initiatives to increase cybersecurity collaboration. The CSDE has led more than 20 cybersecurity and technology organizations to develop the broadest industry consensus on IoT security worldwide, a significant step toward an international standard.



SMB CYBERSECURITY SURVEY

USTelecom's Cybersecurity Survey of Small and Medium-Sized Businesses (SMBs) examines the cybersecurity risks, readiness, and realities that SMBs who own, operate, or support U.S. critical infrastructure face in establishing and maintaining cybersecurity in their organizations.

The first survey, to be published shortly, includes responses from employees, directors/managers, and executives of SMBs with up to 2,500 employees. The survey also includes interviews with approximately 15 SMB Chief Executive Officers (CEOs) to better understand their decision-making process.