BSA's 2025 Global Cyber Agenda

The Enterprise Technology Sector's Agenda for a Secure and Resilient Digital Ecosystem

Cybersecurity is a foundation of a trusted, safe, and modern economy. The leading business software companies work together with governments and stakeholders around the world to achieve our shared goal of better cybersecurity and a more resilient digital ecosystem.

BSA's 2025 Global Cyber Agenda outlines policy recommendations to elevate, improve, and integrate better cybersecurity into all our organizations. Our digitally connected systems are central to our economy and daily lives; that is why it is crucial for organizations to leverage the most effective technologies, like artificial intelligence (AI), to develop the most effective and secure products and services and deploy them throughout the entire digital ecosystem.

Laws and policies should always prioritize cybersecurity and resilience over politics and protectionism. Experience has shown that we can best achieve our shared goals through establishing and expanding public-private partnerships, using risk-based approaches, and leveraging internationally recognized standards and best practices.

BUILDING ON THESE APPROACHES, BSA RECOMMENDS STAKEHOLDERS FOCUS ON ACTIONS TO:

Enhance Software Security

Elevate and Improve Cybersecurity Risk Management

Collaborate Across Borders

Invest in Long-Term Digital Resilience

Enhance Software Security

By driving demand for software developed using secure software development best practices and AI for secure software development, the cybersecurity community will improve the security of products and the resilience of the digital ecosystem through rewarding companies that deliver secure, best-of-breed solutions to customers.

By assuring safe harbor from liability for software producers that use best practices for secure software development, like The BSA Framework for Secure Software, governments will drive all software producers to use secure software development best practices, and thereby improve the security and resilience of the digital ecosystem.

Elevate and Improve Cybersecurity Risk Management

By ensuring cybersecurity laws and policies remain technical and not political, governments provide local businesses and government agencies access to the most effective and secure products and services.

By elevating cybersecurity risk management to boards of directors and executives, organizations can compete on security and trust while delivering value to their customers and communities. For more information see BSA's Cybersecurity for the C-Suite: A Guide to Managing Cybersecurity Risk for Board Members and Executives.

By embracing AI to bolster cybersecurity, including using AI to develop more secure code, detect and respond to threats, and analyze activity and generate threat intelligence, governments will enable cyber defenders to fight on an equal playing field against malicious actors who may try to inappropriately or illegally use AI for malicious purposes. For more information see AI for Cybersecurity.

By developing better cybersecurity metrics, the cybersecurity community will help organizations understand the threats and risks and deploy resources to manage cybersecurity risk more efficiently and effectively.

Collaborate Across Borders

By harmonizing cybersecurity laws and policies internationally, as well as domestically, and accepting the reporting requirements, reports, and certifications of other countries on issues including cyber incident reporting, procurement, and software bills of materials (SBOMs), like-minded countries will ensure industry partners compete on their ability to provide the most effective and secure solutions, rather than their ability to navigate unique or arcane requirements. Governments can most efficiently and effectively achieve this goal by leveraging best practices and internationally recognized standards.

By ensuring data flows across borders and avoiding localization requirements which ultimately undermine cybersecurity and resilience, governments can improve cybersecurity within their borders and around the globe. The security of information is mainly a function of the security controls applied to that information and by allowing data to flow across borders, governments increase security and resilience, including through improved threat detection and response, fraud prevention, and AI-based cybersecurity capabilities.

Invest in Long-Term Digital Resilience

By progressing from legacy to modern IT—and by leveraging innovative technologies like AI and cloud-native security solutions, as well as approaches like multi-cloud—organizations, including government agencies, can make use of best-of-breed solutions and better and more securely serve their customers and citizens.

By transitioning to post-quantum cryptography, organizations will protect their citizens and customers information and prepare themselves to harness the power of quantum computers.

And by building a cyber workforce, through education and training as well as promoting alternative paths to careers (e.g., apprenticeships, boot camps, retraining programs), governments and industry will fill good paying jobs, drive economic growth, and improve cybersecurity and resilience.