Securing Tomorrow: BSA's Cybersecurity Priorities and Software's Essential Role

Around the world, software is driving innovative breakthroughs for governments, businesses, and citizens. Technologies behind the Internet of Things (IoT), 5G telecommunications networks, and cloud computing services are connecting people and organizations in new and transformative ways. These technologies are building connected communities and supporting a vibrant global digital ecosystem.

To preserve the promise of this technological innovation, governments and businesses must work together to ensure its security. The rapidly growing digital ecosystem faces increasingly complex risk, including large-scale data theft, privacy violations, phishing scams, ransomware, and malicious information operations that affect millions of people globally each year. Cybercrime costs trillions of dollars a year, hampering economic growth and threatening jobs. Beyond the financial costs, these threats erode trust in the online environment, disrupt global commerce, and cause physical damage to critical infrastructure, ultimately putting lives at risk.

Effective cybersecurity policies are vital to strengthening international security, preserving trust in the digital economy, and building smart, resilient communities in which individuals and businesses can harness the full benefits of technological innovation. Raising the bar for security practices across the software industry will limit vulnerabilities that malicious actors can exploit; concurrently, many of the most vexing security challenges can be mitigated by innovative software solutions.

BSA | The Software Alliance urges governments to embrace software solutions, as well as collaboration with the software industry, to confront urgent security challenges. Although businesses, private citizens, and government agencies all share responsibility for enhancing cybersecurity, governments play a primary role in advancing global standards, regulations, and market incentives. BSA thus asks governments around the world to expand and harmonize efforts to strengthen cybersecurity through robust public-private collaboration and broad-based international cooperation.

PRINCIPLES FOR EFFECTIVE CYBERSECURITY

Cybersecurity policy solutions will be most effective when they:

• • •

Embrace public-private collaboration

• • •

Foster market-driven solutions

• • •

Protect user privacy

• • •

Build or sustain international consensus

• • •

Are risk-based, adaptable, and outcome-oriented

More specifically, we strongly support a robust partnership of government and industry to:

Promote **a secure software ecosystem** by leveraging industry standards, developing novel tools to understand critical security information, and strengthening security research and vulnerability disclosure.

Advocate collaborative approaches to **strengthen supply chain security** by supporting interoperable, risk-based supply chain security policies, strengthening security of 5G and software supply chains, and prioritizing cybersecurity in government acquisition.

Pursue **international consensus for cybersecurity action** by supporting international standards development as well as working to align international security laws and promote agreement on global norms.

Develop a **21st century cybersecurity workforce** by increasing access to computer science and STEM education, opening new paths to cybersecurity careers, and empowering workers with technology.

Advance cybersecurity by **embracing digital transformation**, advancing innovative cloud security solutions, leveraging the potential of emerging technologies, and forging innovative partnerships to combat emerging risks.

Working together, government and industry can help the world's citizens reap the benefits of the digital economy while protecting our safety, security, and privacy.

Key Elements of BSA's Cybersecurity Agenda

Promote a Secure Software Ecosystem

» **Establish the *BSA Framework for Secure Software* as a widely recognized benchmark for software security.** Support adoption of a set of widely recognized, industry-driven software development and management best practices to elevate cybersecurity methods and promote resiliency.

» **Develop novel tools to communicate critical cybersecurity information to consumers and enterprise stakeholders.** Establish widely used, market-driven tools for providing relevant cybersecurity information to consumers and enterprise stakeholders to inform purchasing decisions, network operation, and risk management.

» **Strengthen identity management.** Work to expand adoption of identity management technologies across public and private sector organizations, and to increase emphasis on identity management in cybersecurity policies and frameworks.

» **Promote security research and vulnerability management.** Strengthen investment in security research aligned to coordinated vulnerability disclosure programs, and drive adoption of coordinated vulnerability disclosure by governments and businesses.

» **Drive IoT cybersecurity by adopting proven software security best practices.** Integrate security-by-design principles into IoT standards and guidance, and develop frameworks for assessing risk and identifying security measures.

Advocate Collaborative Approaches to Strengthen Supply Chain Security

» **Secure information technology supply chains through interoperable, risk-based policies.** Strengthen supply chain security for information technology products by establishing holistic, transparent, fair policies that prioritize risk management and public-private collaboration.

» **Strengthen security of software supply chains.** Advance innovative approaches to managing third-party and open source software components.

» **Drive security in 5G and future networks.** Promote adoption of software solutions to 5G security challenges, undergirded by internationally recognized standards and multilateral approaches to governance.

» **Prioritize cybersecurity in government acquisition.** Incentivize cybersecurity by creating competition for cybersecurity performance in government acquisition processes.

Pursue International Consensus for Cybersecurity Action

» **Align global cybersecurity laws to promote security and economic growth.** Support both cybersecurity and economic growth by promoting the alignment and international interoperability of laws and policies across countries to foster innovation, security advancements, free flows of data, and market access.

» **Advance international cybersecurity norms.** Encourage international dialogue and drive agreements on cybersecurity practices in bilateral and multilateral frameworks.

- **Support international standards development and adoption.** Support efforts to develop and update international standards for key security functions. Encourage global adoption of policies and certification frameworks aligned with international standards.
- **Build international capacity for good cyber governance.** Work with governments to expand global efforts to build international capacity for cyber governance and contributions to global stability in cyberspace.

Develop a 21st Century Cybersecurity Workforce

- **Increase access to computer science education.** Expand cybersecurity and STEM education for K–12 as well as in undergraduate computer science programs, increase scholarships, and encourage diversity.
- **Promote alternative paths to cybersecurity careers.** Launch careers through apprenticeship programs, community colleges, "boot camps," and public service, and establish mid-career retraining programs to provide workers with high-demand cybersecurity skills.
- **Leverage automation to empower workers.** Accelerate adoption of technologies that help cybersecurity professionals more effectively identify risks and focus on high-priority tasks.
- **Build a highly skilled workforce to defend the most critical systems.** Target training and education programs to meet demands for cybersecurity professionals to defend information and operational technologies underpinning critical infrastructure.

Advance Cybersecurity through Digital Transformation

- **Advance innovative solutions to cloud security.** Support widespread adoption of cloud technologies by advancing standards-based cloud security policies that enable innovative, adaptable security solutions.
- **Help Smart Cities stay cyber resilient.** Provide planning support, threat information, and incident response support to municipal planners and managers to enhance the resilience of Smart Cities against cyber threats. Encourage national governments to provide funding and other support to local governments for Smart Cities cybersecurity.
- **Leverage emerging technologies to enhance security.** Target investments and constructive policies to capitalize on the tremendous potential of artificial intelligence, quantum computing, blockchain, strong encryption, and other emerging technologies to enhance security.
- **Modernize government IT.** Invest in IT infrastructure for governments at all levels with an eye toward cybersecurity, including through adoption of cloud computing, defense-in-depth, continuous monitoring, and innovative security technologies.