BSA's 2024 Global Cyber Agenda

Digital transformation, the integration of digital technologies into all aspects of an organization's operations, is more important than ever. People around the globe enjoy the benefits of digital transformation by using trusted enterprise technology platforms to work, learn, run businesses, and stay connected.

However, malicious actors continue to attempt to undermine the digital ecosystem for financial or other gain. And there is no sign these malicious efforts will abate.

Strong cybersecurity risk management enables digital transformation and protects the underlying information produced or provided by organizations and people.

Experience has taught us that the most effective laws and policies actively:

- Build on public-private partnerships.
- Use risk-based approaches.
- Leverage internationally recognized standards and best practices.

Effective policies also avoid elevating politics and protectionism over cybersecurity. When policymakers use cybersecurity to justify protectionism, they increase risks to customers who have limited access to best-of-breed services and undermine the security of the entire digital ecosystem.

To achieve the best results for the entire digital ecosystem, the cybersecurity community, including policymakers around the world, should focus their efforts on five priority areas.

1 Enhancing Software Security

- **Use AI to Improve Secure Software Development.** Software producers should leverage AI to improve the secure software development process, including by identifying and remediating vulnerabilities.
- **Align AI and Software Risk Management Guidance.** Security guidance for AI systems should be framed as complementary to existing guidance for software security practices and provide risk-based, implementation-agnostic practices to address unique AI concerns, taking steps to avoid contradictions or redundancies.
- **Incentivize Risk-Based Approaches Leveraging Best Practices With a Safe Harbor From Liability.** Industry and governments should explore developing safe harbors from liability for software producers that use best practices for secure software development.
- **Pursue Strategic Adoption to Address Memory Safety.** All stakeholders should pursue a policy of strategic adoption, which requires active risk management; sets a bold but achievable path to a more secure future; prioritizes new code; invests in research and development; provides training and support; deploys incentives; and has governments leading by example. For more information, see Memory Safety: A Call for Strategic Adoption.
- **Expedite Incident Response With Usable Software Bills of Materials (SBOMs).** Industry and governments should continue to work to standardize SBOMs. SBOMs are not a panacea, but can expedite incident response once customers are prepared to use them. For more information, see SBOMs: Considerable Progress, But Not Yet Ready for Codification.

ARTIFICIAL INTELLIGENCE

Artificial intelligence (AI) is a transformative technology that will impact all sectors of the economy. AI has the potential to improve cybersecurity, and policies should support:

- **Using AI to improve secure software development.**
- **Harnessing AI to improve cybersecurity risk management.**
- **Deploying AI to meet today's challenges with today's solutions.**

2 Improving Cybersecurity Risk Management

» **Harness AI to Improve Cybersecurity Risk Management.** Policymakers should ensure that cyber defenders can use AI to keep pace with malicious actors and improve defenses. For more information see AI for Cybersecurity: Ensuring Cyber Defenders Can Leverage AI to Protect Customers and Citizens.

» **Build a Digital Identity Ecosystem.** Industry should continue to build and improve, and government should leverage, cloud-native, scalable, and interoperable digital identity solutions that enable zero-trust architectures, including by using phishing-resistant, multi-factor authentication.

» **Enable Cross-Border Data Flows.** Like-minded allies should ensure the free flow of data across borders, without which cyber defenders will be unable to monitor traffic patterns, identify anomalies, and respond to risks. Furthermore, policymakers should recognize that data localization requirements generally decrease an organization's resilience and make it vulnerable to risks such as invasions or natural disasters.

» **Improve Cloud Security and the Shared Responsibility Model.** Cloud service customers (including government agencies) and cloud service providers should use best practices to manage their shared responsibility to secure cloud services and make them resilient.

» **Accelerate Adoption of Post Quantum Cryptography.** Policymakers should accelerate investments in, and promote the adoption of, quantum-resistant cryptography that is necessary to safeguard data now and into the future, including by developing strategies and working with like-minded allies to build a resilient quantum-ready digital ecosystem.

3 Investing in Modern Information Technology

» **Procure Commercial Solutions.** Governments should continue to prefer commercial-off-the-shelf solutions, including as shared services, rather than government-developed products that relegate government agencies to technology that will not keep pace with innovation.

» **Leverage Cloud Computing and Multi-Cloud Solutions.** Governments and businesses should modernize IT systems by adopting cloud services generally to enhance security and resiliency of their organizations. Furthermore, policymakers should support adopting multi-cloud architectures that promote choice, interoperability, interconnectivity, and open data.

» **Capitalize on the Opportunity to Improve Cybersecurity.** Governments should use the transition to cloud services as an opportunity to analyze potential security gaps and leverage cloud-native security solutions to bridge those gaps.

» **Deploy AI to Meet Today's Challenges With Today's Solutions.** Governments and businesses must invest in AI-driven cybersecurity solutions to keep pace with malicious actors who are already using AI to improve their exploits.

» **Support Cybersecurity at Every Level of Government.** The entire cybersecurity community must work together to address the challenges faced at every level of government—from national to municipal—each of which face similar threats, but some of which have tighter resource constraints.

4 Harmonizing and Making Reciprocal Laws and Policies

» **Make Requirements Consistent Within and Between Governments.** Policymakers should require the various government agencies to harmonize their cybersecurity requirements based on internationally recognized standards; they should incentivize harmonization across local jurisdictions; and they should engage internationally to harmonize requirements among like-minded allies.

» **Accept Certifications, Reports, and Similar Artifacts from Like-Minded Allies.** Policymakers should drive consistency and interoperability, as well as reduce redundancy by leveraging internationally recognized standards for cybersecurity certifications, and further accept as sufficient the certifications, reports, and other similar artifacts from like-minded allies and local jurisdictions.

5 Building the Workforce of the Future

» **Invest in Education and Training.** Industry and governments should provide opportunities to all members of society by increasing the accessibility of education and training as well as promoting alternative paths to careers (e.g., apprenticeships, boot camps, retraining programs).