The Software Alliance
BSA

Enhancing Cyber Policy, Advancing Digital Transformation

BSA'S 2023 GLOBAL CYBER AGENDA

Cybersecurity is growing in importance as organizations of all types continue their digital transformations. Governments rely on cybersecurity to protect critical services delivered to citizens, businesses rely on cybersecurity to ensure trust in products, and we all rely on cybersecurity to connect to our family, friends, and communities.

Cyber Policy North Stars

Prior to developing, enacting, and implementing laws and policies, policymakers should choose the tool best suited to address a cyber challenge, which may sometimes be a new law or policy, but may often be increased focus and resources on building and improving the operational capacity of the international community, country, sector, or organization.

Additionally, policymakers should consider the different roles played in securing products and services throughout the ecosystem. Even within the tech sector, there are a range of companies involved in delivering services. For example, the enterprise tech sector sells businesses and governments the solutions they need to be competitive and effective, including cloud computing, customer relationship management; human resources management; identity, credentialling, and access management; data analytics; manufacturing; and infrastructure tools and services.

If policymakers determine that laws and policies are needed to address a particular challenge and have effectively targeted them, then policymakers should keep in mind the following cyber policy north stars as they chart a path forward.

CYBER POLICY NORTH STARS

Encourage Public-Private Collaboration

Support Integrated Risk-Based Approaches

Incentivize Innovation

Limit Cybersecurity Policies to Cybersecurity Purposes

Encourage Public-Private Collaboration

Policymakers can increase the likelihood that a law or policy achieves their intended outcome, while minimizing unintended consequences, by acting transparently and collaborating with industry to add clarity to policies. **In a world in which neither industry nor government alone can solve an ever-evolving set of challenges, public-private partnerships have proven to be the most effective approach to improving the cybersecurity of both organizations and the digital ecosystem.**

Support Integrated Risk-Based Approaches

Laws and policies that support risk-based approaches, built on internationally recognized standards, offer the most direct path toward improved cybersecurity and a more secure digital ecosystem. **Returning to the prescriptive, compliance-based checklists of the 20th century will provide malicious actors more opportunities to launch successful cyber attacks.** Years of effort to elevate cybersecurity risk management to the C-suite will be lost if governments provide prescriptive checklists.

Incentivize Innovation

Outcome-based laws and policies incentivize companies to develop new, better, and more cost-effective technologies to achieve the desired outcome. Such policies have the added benefit of increasing the likelihood that a law or policy can accommodate a new technology. In contrast, **when policymakers codify prescriptive actions, they remove the incentive for companies to innovate more efficient and effective ways to achieve the same or improved cybersecurity outcomes.** If certain requirements are prescribed, the relevant laws or policies should clarify that such rules constitute minimum necessary actions—floors, not ceilings—to ensure continued advancement and avoid inefficacy in the face of evolving threats.

Limit Cybersecurity Policies to Cybersecurity Purposes

Policymakers should ensure that cybersecurity laws and policies are focused on cybersecurity and not used for other policy objectives. Many countries are considering or implementing laws and policies, such as data localization, that are described as cybersecurity laws, but do not enhance cybersecurity; rather, they use cybersecurity to justify protectionist outcomes. **By elevating politics and protectionism over cybersecurity, policymakers harm the cybersecurity of organizations and the digital ecosystem.**

BSA's Cybersecurity Policy Priorities and Recommendations

Priority: Improving Software Security

BSA supports improving the security of software by leveraging best practices, like the BSA Framework for Secure Software, and internationally recognized standards.

» Policymakers should encourage software developed by their governments (including software developed through contractors) and vendors to use secure development practices, build in secure capabilities, and manage risk to software throughout its lifecycle.

» Policymakers should require software developed by their government or its contractors to meet the same security standards it requires of its vendors.

BSA supports developing and using software bills of materials (SBOMs) as well as the associated tooling, standards, and automation necessary for transforming the information contained in an SBOM into concrete cybersecurity improvement. But as explained in our blog SBOMs: Considerable Progress, but Not Yet Ready for Codification, BSA cautions policymakers that SBOMs alone will not address most, let alone all, of the daily cyber risks an organization faces, and they need to be integrated into a broader supply chain risk management strategy that can deliver and use them.

» Policymakers should support the development of SBOMs and related materials by avoiding prematurely codifying SBOM requirements or developing their own regional or national standards, and instead encourage the fast-paced and productive collaboration between the software industry, government, and other stakeholders to develop SBOMs, associated materials, and internationally recognized standards.

BSA supports organizations developing and maintaining coordinated vulnerability disclosure programs. Vulnerability disclosure is a particularly complex cybersecurity challenge. National or regional vulnerability disclosure laws and policies that diverge from internationally recognized standards will make the entire digital ecosystem less secure.

» Policymakers should support organizations developing, maintaining, and using vulnerability disclosure programs based on internationally recognized standards, not national or regional vulnerability disclosure laws and policies.

Priority: Managing Cybersecurity Risk for Emerging Technologies

BSA supports building in risk-based cybersecurity from the beginning of the design process to help ensure emerging technologies like artificial intelligence (AI), 5G, and quantum computing bring broad transformational benefits to society.

» Policymakers should prioritize securing, building, and harnessing 5G networks including by supporting open radio access networks (ORANs) that support security and resilience; managing spectrum, promoting competition, and supporting the delivery of carrier-grade cloud solutions; taking a risk-based approach to securing AI systems, including focusing efforts on high-risk systems used as input to consequential decisions; integrating AI into cybersecurity programs, for example, supply chain risk management and vulnerability databases; and preparing to manage the risks created by quantum computing, including by supporting the standardization and implementation of quantum resistant cryptography.

Priority: Harmonizing Laws and Policies Within and Between Governments

BSA supports laws and policies that concretely improve cybersecurity, and that are based on best practices and internationally recognized standards. Supply chains are global and products contain components from numerous jurisdictions. By building laws and policies on top of internationally recognized standards, policymakers can support overall product security and supply chain resilience. In contrast, cybersecurity requirements or other certifications that are unique to a region or country are frequently non-tariff trade barriers masquerading as a commitment to cybersecurity, and degrade the security of organizations and the digital ecosystem.

- Policymakers should align cybersecurity laws and policies to ensure consistency and harmonization across government agencies and sectors.
- Policymakers should work internationally to harmonize requirements so that vendors are selected based, not on having the largest compliance team, but on the security and functionality of the solutions they offer.
- Policymakers should not rely on domestic certifications but rather should use internationally recognized standards and accepted certifications from internationally accredited bodies as demonstration that a vendor has implemented appropriate security controls, and should consider recognizing certifications accepted by like-minded allies as demonstration of a vendor's security practices.

Priority: Investing in Modern IT Infrastructure and Cybersecurity

BSA supports increased investment in modern IT infrastructure and cybersecurity, for example by migrating to cloud services and leveraging multi-cloud; implementing zero trust architecture; and using state-of-the-art identity, credentialling, and access management.

- Policymakers should invest in modern IT infrastructure and cybersecurity commensurate with the risk, including supporting regional, state, local, or municipal governments to improve their cybersecurity. Organizations, including governments, should expect these investments to grow as they continue their digital transformations, and thus are able to deliver better, more secure services to citizens and customers.
- Policymakers should make or reiterate their commitments to using commercial-of-the-shelf (COTS) solutions over government-produced products. Enterprise technology companies continuously update their solutions to improve both security and functionality. Relegating government agencies to products that have a track record of becoming obsolete is short-sighted and will result in worse services for citizens.

Priority: Developing the Workforce of the Future

BSA supports increased investment in the workforce necessary to deliver on the promise of digital transformation. Fortunately, the challenge of developing the workforce of the future is also an opportunity to provide good-paying jobs, not just for people with graduate or post-graduate degrees, but to people of all ages and backgrounds.

- Policymakers should make significant investments in broadening opportunities, promoting alternative paths (e.g., apprenticeships, boot camps, retraining programs), improving training programs, and expediting the development of the diverse workforce necessary to secure our shared future.