BSA The Software Alliance

THE BUILDING BLOCKS OF A STRONG LEGAL CYBERSECURITY FRAMEWORK

Construct Solid Legal Foundations

Governments should enact and keep up-to-date a comprehensive legal and policy framework, based on a solid national cybersecurity strategy. This framework should be built upon the following key principles.

- **Risk-based and prioritised:** Cyberthreats come in many shapes and magnitudes with varying degrees of severity. Establishing a hierarchy of priorities — based on an objective assessment of risk — with critical assets and/or critical sectors at the top is an effective starting point from which to ensure that cyber protections are focused on those areas where the potential for harm is greatest.
- **Technology-neutral:** A technology-neutral approach to cybersecurity protection is vital to ensure access to the most secure and effective solutions in the marketplace. Specific requirements or policies that mandate the use of certain technology only undermine security by restricting evolving security controls and best practices, and potentially creating single points of failure.
- **Practicable:** Any strategy is only as effective as it is adoptable by the largest possible group of critical assets, and implementable across the broadest range of critical actors. Overly burdensome government supervision of private operators, or disproportionately intrusive regulatory intervention in their operational management of cybersecurity risk, would most often prove counterproductive, diverting resources from effective and scalable protection to fragmented administrative compliance.
- **Flexible:** Managing cyber risk is a cross-disciplinary function and no "one-size-fits-all" approach exists. Each industry, system and business faces distinct challenges, and the range of actors must have flexibility to address their unique needs.
- **Respectful of privacy and civil liberties:** Security requirements should be duly balanced with the need for protection of privacy and civil liberties. Ensuring that requirements and obligations are proportionate, do not represent more intrusion in fundamental rights than what is strictly necessary, follow due process and are supported by adequate judicial oversight all are important considerations to address in any cybersecurity framework.

Establish Operational Entities with Key Responsibilities for Security

Governments should set up operational entities to support the prevention of cybersecurity incidents and ensure response to them. A core component of this is the establishment of operational computer security, emergency and incident response teams.

Engender Trust and Work in Partnership

No country or government can address cybersecurity risk in isolation. Collaboration with non-governmental entities as well as with international partners and allies is a crucial component of an effective approach to cybersecurity.

- **Partnering with the private sector:** Most infrastructure is owned by the private sector, making effective public-private cooperation essential. Cooperation also improves the effectiveness of risk management by improving the sharing of information, experience and perspective of multiple sources. Particular efforts are needed to foster trust and avoid legal obstacles that may hinder it.
- **Global rather than isolated:** Given that cyberthreats are global, effective cybersecurity policies and strategies need to maintain an international outlook, and build on joint efforts with partners and allies. They should also leverage international, voluntary and market-driven standards in order to maximize pan-regional and global information sharing and protection.

Foster Education and Awareness About Cybersecurity Risk

People, process and technology are equally important to ensuring cybersecurity. Even the best technology will be ineffective if not used appropriately. Awareness raising, education and training about clearly articulated cybersecurity priorities, principles, policies, processes and programs are essential components of any cybersecurity strategy.