Business Software Alliance

BSA 2026 Global Cyber Agenda

Innovating to Meet and Defeat Evolving Cyber Threats

The rapid adoption of artificial intelligence (AI) is driving innovation, reshaping risk, and strengthening cyber defenses, while rising geopolitical tensions and state-sponsored actors are among the drivers of increased malicious activity. In an era of rapid change, the one certainty is that cyber threats will continue to evolve, which is why laws and policies must remain flexible and outcome-focused.

To deliver for citizens and customers, governments and industry must work together to build a secure and resilient digital ecosystem. Lasting progress requires we build on a strong foundation that understands cybersecurity as a shared responsibility and strengthens public-private partnerships; keeps cybersecurity technical, not political; recognizes that threats cross borders, making international cooperation imperative; and leverages risk-based approaches as well as internationally recognized standards and best practices.

These foundations underscore the need for clear priorities to ensure that our efforts remain effective, efficient, and mutually reinforcing.

BSA RECOMMENDS GOVERNMENTS AND INDUSTRY FOCUS ON

- **Harnessing and Securing AI**
- **Harmonizing and Simplifying Regulations**
- **Modernizing Legacy Systems and Upgrading to Post-Quantum Cryptography (PQC)**
- **Creating a Global Ecosystem that Delivers Secure Innovation**
- **Achieving Measurable Security Outcomes**

Harnessing and Securing AI

AI is already a critical tool for strengthening cybersecurity. It helps, among other activities, dramatically improve, expedite, and automate identification, detection, and response. By adopting AI-enhanced cybersecurity solutions, organizations can better manage a rapidly evolving risk environment and stay ahead of adversaries. Additionally, organizations should use available AI tools to identify and then secure their AI systems and enable AI adoption.

Harmonizing and Simplifying Regulations

Governments have been proposing and adopting cyber regulations that do not work together in a coherent manner. Duplicative and fragmented regulations, like those often found in cyber incident reporting and cloud certification schemes, add complexity without improving security. By ensuring coordination across government agencies, building on internationally recognized standards, and pursuing mutual recognition, we can reduce burdens, foster innovation, and achieve better security outcomes.

Modernizing Legacy Systems and Upgrading to Post-Quantum Cryptography (PQC)

Outdated and bespoke IT systems, especially in government, are increasingly unable to meet citizens' needs while withstanding sophisticated threats. These legacy systems also lack the capacity to support PQC, which already renders data vulnerable to "harvest now, decrypt later" attacks. By modernizing IT environments, including migration to secure cloud platforms, we can prepare to upgrade to PQC while simultaneously improving service delivery, security, and resilience.

Creating a Global Ecosystem that Delivers Secure Innovation

The best way to meet evolving threats is to foster a marketplace that prioritizes secure innovation, not just first to market. Governments should incent investments in the foundations of a resilient digital economy. These foundations include leveraging secure software development best practices and scalable cloud services, promoting the use of open standards, and avoiding trade barriers disguised as security requirements, like data localization mandates. By providing these incentives, governments can encourage the next generation of security innovations.

Achieving Measurable Security Outcomes

Laws and policies should focus on measurement that drives concrete security improvements, not on rewarding bureaucratic activity or box-checking. To ensure value, policies should use metrics like "mean time to detect" and "mean time to respond," while developing additional consensus metrics as needed. Just as medical professionals rely on vital signs, governments and businesses should establish and adopt cyber vital signs to pinpoint challenges, such as fragmented environments and overlapping tools that create blind spots and slow incident response. These shared metrics can help organizations streamline operations, accelerate threat detection and response, enable meaningful comparison, increase returns on security investment, and drive continuous improvement.