For Immediate Release

Media Contact:
Tom Knock, James Baines
bsa@brands2life.com

BSA Survey of EU Cybersecurity Laws Identifies Gaps in Member States' Cyber-Preparedness

London, UK — 24 February 2015 — A first-ever analysis of cybersecurity laws and policies in Europe finds gaps and fragmentation in Member States' cyber preparedness.

The report, released today by BSA | The Software Alliance, evaluates national laws, rules and policies in all 28 EU Member States against 25 criteria deemed essential for effective cybersecurity protections. It is intended to provide EU Member States with an opportunity to evaluate their countries' policies against key metrics and maps a way forward by outlining the key building blocks for a strong cybersecurity legal framework.

"There is an uneven landscape when it comes to cyber protections across Europe. Most Member States acknowledge cybersecurity to be a priority, yet inconsistencies in their approach leave the entire Single Market vulnerable to threats," said Thomas Boué, BSA's director of policy – EMEA. "The Network and Information Security Directive could help to establish a stronger foundational level of cybersecurity and cyber resilience if it focuses on aligning the preparedness of Europe's most critical infrastructure and introduces harmonised reporting and information sharing processes throughout the Single Market."

Among the key findings of the report:

- Most EU Member States recognise cybersecurity to be a national priority – particularly with regard to critical infrastructure.
- Considerable discrepancies exist between Member States' cybersecurity policies, legal frameworks and operational capabilities, resulting in notable gaps in overall cybersecurity protections in Europe.
- Nearly all EU Member States have established incident response teams to address cyber incidents; however, the mission and experience of those entities varies.
- There is a worrying lack of systematic public-private cooperation and collaboration on cybersecurity between EU governments and non-governmental entities and international partners.

- The UK has a comprehensive cybersecurity strategy, released in 2011. It is complemented by a strong cybersecurity legal framework and two computer emergency response teams: CERT-UK which supports operators of critical infrastructure and GovCertUK which supports government agencies. Other relevant bodies include the National Security Council and the Office of Cyber Security and Information Assurance.
- The UK also has a well-developed system of public-private partnerships in which the private sector actively participates – a collaboration strongly supported by its cybersecurity strategy.

The report encourages EU Member States to focus on four key elements of a strong legal cybersecurity framework:

- Construct and maintain a comprehensive legal and policy framework based on a national cybersecurity strategy that is complemented by sector-specific cybersecurity plans.
- Establish operational entities with clear responsibilities for operational computer security, emergency and incident response.
- Engender trust and work in partnership with the private sector, NGOs and international partners and allies.
- Foster education and awareness about cybersecurity risk and priorities.

At the same time, the report cautions European governments to avoid unhelpful protectionist regimes that can undermine, rather than improve, cybersecurity protections. Specifically, Member States should:

- Avoid unnecessary or unreasonable requirements that can restrict choice and increase costs including unique, country-specific certification or testing requirements; mandates for local content; requirements to disclose sensitive information, such as source code or encryption keys; and restrictions on foreign ownership of intellectual property.
- Refrain from manipulating standards, instead supporting industry-led, internationally recognised technical standards.
- Avoid data localisation rules and ensure the free-flow of data across markets.
- Steer clear of preferences for indigenous technologies which obstruct foreign competition and harm global innovation.

The full 28-country report, as well as detailed summaries for each EU Member State, are available at www.bsa.org/EUcybersecurity.

About BSA

BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 60 countries around the world, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.