THE POSITIVE AGENDA FOR GLOBAL CYBERSECURITY:

Join the Private Sector Taking Action to Reduce Global Cyber Risk

Join a network of leading technology firms, trade associations & governments worldwide working to define global cybersecurity policy through the Positive Agenda.

TECH ACCORD

The Positive Agenda priorities include:

- Developing global private sector cybersecurity policy objectives;
- Working with firms and governments on practical action to reduce global risks and increase cyber defenses;
- Protecting innovation and IP and increase trust amongst responsible actors; and
- Promoting robust cross-border public-private cyberthreat information sharing.

By participating in the Positive Agenda, you will secure a seat at the table proactively defining global priorities to address cybersecurity threats before those decisions are made for you.

The Positive Agenda for Global Cybersecurity

Global cyber-insecurity is rapidly growing. Ransomware, attacks on critical infrastructure, and data breaches, are becoming increasingly common, and current trends are moving in a negative direction. There is no effective international response mechanism to address cyberattacks, nor is there a comprehensive plan to resolve these issues. Furthermore, industry has yet to clearly articulate its priorities for reducing global cyber risk. The Positive Agenda for Global Cybersecurity is the answer to this gap through partnership with firms, trade associations, and governments worldwide.

The Positive Agenda for Global Cybersecurity is an initiative born from the Cybersecurity Tech Accord, a global technology alliance of over 160 firms, which has partnered with international organizations and governments since 2018 on cybersecurity policy. To address the rapidly increasing threat landscape the Tech Accord launched this campaign and is offering a seat at the table in pursuing global cybersecurity action.

What's at Stake

Russia and China are advancing proposals to increase state control over information technology—Russia through an ICT treaty and China via a data-sovereignty agenda. If adopted, these measures would impose binding obligations on private companies, especially Western firms, and undermine their competitiveness. **Even if your home jurisdiction doesn't join such agreements, you would still need to comply in international markets that do.**

For businesses, the risks are significant: forced technology transfers, new liabilities for multinational ICT providers, limits on independent cyberattack attributions, mandated encryption backdoors and restrictions on AI development.

The private sector faces a choice—work with like-minded partners to drive global cyber risk reduction or play defense in negotiations aimed at marginalizing Western firms in global markets.

apco

Take Action & Get Involved:

Scan to learn more and register your interest by contacting **Nick Ashton-Hart** of APCO at nashtonhart@apcoworldwide.com