

Top Risks in Cybersecurity 2023

The United States is facing increasing cybersecurity risks, posing significant threats to businesses and individuals alike. Identifying these risks is crucial so policymakers and businesses can take pragmatic action and invest in countermeasures. The Bipartisan Policy Center, in collaboration with Equifax and a group of expert advisors, has identified the top cybersecurity risks facing the nation in 2023.



Evolving Geopolitical Environment

Increasing international conflicts have led to a rise in cyberattacks that will require continued attention and countermeasures in 2023.



Accelerating Cyber Arms Race

The ever-evolving cyber landscape and advances in technology require defense against old and new attacks in an ongoing arms race.



Global Economic Headwinds

In economically uncertain times, difficult investment and resource allocation decisions could lead to unintended cybersecurity risks, especially for startups and small and medium sized businesses.



Overlapping, Conflicting, and Subjective Regulations

A patchwork of cybersecurity and related data and privacy laws create barriers for companies navigating these regulations, creating a desire for a more coherent and flexible approach to regulation.



Lagging Corporate Governance

The corporate sector faces significant vulnerabilities in managing cyber threats due to limited communication between security professionals and leaders and insufficient technical expertise on boards.



Lack of Investment, Preparedness, and Resilience

Insufficient preparation, testing of operational resiliency, and investments in up-to-date technology leave the public and private sector vulnerable to cyberattacks and emerging threats.



Vulnerable Infrastructure

Critical infrastructure faces unique cybersecurity threats, and the public and private sector share responsibility for securing essential services, which are critical to daily life.



Talent Scarcity

The shortage of trained cybersecurity professionals and the excess demand for more highly skilled professionals, poses a significant risk to organizations as the demand for cyber modernization grows.