COVID-19 accelerated the use of biometric data collection systems.

Companies that allowed employees to work from home created new privacy and cybersecurity vulnerabilities.

The attack on the U.S. Capitol led to an unprecedented amount of cybersleuthing—everyday people finding and posting the identities of insurgents online.

There was a dramatic increase in Internet of Things scams and attacks, as hackers took advantage of employees and students working from their own devices and home networks, which are rarely secure.

75% of businesses do not involve their boards of directors in cybersecurity oversight.

Cyberattacks cost the world economy an estimated $445 billion, or almost 1% of global income, according to the Center for Strategic and International Studies.

Hackers increasingly look for sensitive intellectual property (business communications, vaccine code, DNA records).

Cybersecurity risk areas this year include health care, pharmaceuticals, advanced materials and manufacturing, retail, municipalities, and military technology suppliers.