Cybersecurity Law Basics

What is cybersecurity law?

The statutes, regulations and applied common law doctrines that punish attacks on, allocate liability for, and seek to mandate or otherwise improve the security and resiliency of computers, computer information, and computer-based or computer-controlled systems.

CYBERSECURITY LAW INCLUDES

- → Standards intended to safeguard data and ensure the secure operation of systems and networks.
- → Criminal laws that punish those who attack computer networks and computer data.
- → Requirements to implement organizational and technical measures to protect networks and information from unauthorized access, breaches and cybercrime.
- → Obligations on data custodians to protect personal data against loss or misuse.
- → Laws mandating breach notification and incident reporting to authorities and/or affected individuals to enable quick responses to cyberthreats.
- → Measures to facilitate international cooperation among organizations and governments against cyberthreats not limited by traditional borders.

Much of cybersecurity law is based upon risk management and employs measures such as risk assessments, security audits and incident response planning.

The ultimate goal of cybersecurity law is to protect the confidentiality, integrity and availability of personal information, intellectual property and critical infrastructure.

Cybersecurity law is not limited to

IT SECURITY

Cybersecurity law goes beyond data protection and focuses on the integrity of the operational technology that controls physical processes.

LARGE ORGANIZATIONS

Cybersecurity laws can apply to any organization that handles personal information or maintains digital systems, regardless of size or industry.

PROSECUTING CYBERCRIME

Although cybersecurity law covers cybercrime, it also addresses preventative measures, organizational liability and incident response.

DATA PROTECTION OR PRIVACY

Although it is an element of privacy or data protection, cybersecurity law is broader. It addresses not just how personal information is collected, used and shared, but also the security of all types of data and the operational availability of computer-based or computer-controlled networks and systems.

TECHNICAL STANDARDS

While some cybersecurity laws require organizations to follow specific technical standards, others only require reasonable security. Cybersecurity laws may require management practices, such as risk assessment, access control establishment and response plan adoption, but leave the choice of specific technologies to organizations.

Laws and regulations that impact cybersecurity

Australia's Cyber Security Act 2024

Introduces mandatory security standards for smart devices, establishes reporting obligations for ransomware payments and encourages other voluntary reporting to the government to support responses to significant cyber incidents.

Brazil's General Data Protection Law

Requires appropriate technical and organizational security measures for personal data and authorizes heavy fines for noncompliance.

Data Security Law and Cybersecurity Law of the People's Republic of China

Establish a framework of strict cybersecurity measures, including data localization, influencing how multinational companies manage networks and data operations within China.

EU General Data Protection Regulation

Requires appropriate technical and organizational security measures for personal data and mandates breach notifications.

EU NIS2 Directive

Expands upon the Network and Information Security Directive, requiring service providers and manufacturers in critical sectors to implement specific types of risk management measures and report security incidents.

India's Information Technology Act

Criminalizes cybercrimes such as identity theft, hacking and the spread of malicious software. Establishes the Indian Computer Emergency Response Team to handle cybersecurity incidents.

Nigeria's Cybercrimes (Prohibition, Prevention, Etc.) Act 2015

Criminalizes cybercrimes, mandates registration of cybercafes and grants investigatory powers to law enforcement authorities.

Singapore's Cybersecurity Act 2018

Requires operators of critical information infrastructure to comply with specific types of risk management measures and report cybersecurity incidents. Mandates licensing requirements for cybersecurity providers and grants the Cybersecurity Commission the authority to investigate and respond to threats.

U.S. Cybersecurity Information Sharing Act

Aims to promote voluntary information sharing among private organizations and with the U.S. government regarding cyberthreats and defensive measures.

U.S. Federal Trade Commission Act

Prohibits unfair or deceptive trade practices, which the FTC has interpreted to include deceptive statements about cybersecurity and failure to protect personal information with reasonable security.

Published January 2025.

iapp.org