8 Best Practices for Avoiding Data Breaches*

*Based on Eight Data Security Best Practices Revealed by Recent AG and FTC Enforcement Actions, by Ann-Marie Luciano and Jawaria Gilani, published in *Cybersecurity Law Report*, January 8, 2020.

Analysis of recent state Attorney General and Federal Trade Commission enforcement actions shows that companies should focus on access control, threat awareness and advanced technical security measures.

Access Control

Is your sensitive information protected?

Threat Awareness

Have you assessed your vulnerabilities?

Technical Security

Have you implemented advanced security measures?

Steps You Can Take

ACCESS CONTROL

1. Impose security requirements to protect sensitive information, such as use of 2-factor or multi-factor authentication and password vaults, and hashing (scrambling) of passwords.
2. Limit scope of access to sensitive information to necessary users and regularly review users' privileges.

THREAT AWARENESS

3. Conduct frequent network monitoring and logging.
4. Undertake regular penetration tests and vulnerability scans.
5. Train employees and agents to safeguard sensitive information.

TECHNICAL SECURITY

6. Segment networks to separate where sensitive information is collected, processed, stored or accessed from other sections of the network.
7. Patch software in a timely manner.
8. Encrypt sensitive information before storage or transmission over a network.

Adopting these eight best practices can mitigate the likelihood of a future data breach and help reduce the risk that regulators will find fault in the reasonableness of an organization's data security practices.

To read about major changes the FTC announced in January 2020 to improve data security and deter breaches, click here or visit ftc.gov.

For more information on Cozen O'Connor's State Attorneys General Practice, click here or visit cozen.com/practices-industries.

COZEN O'CONNOR