- **In 2019, 66% of small businesses experienced a cyberattack.**
- **63% of small to medium-sized businesses experienced a data breach involving loss or theft of sensitive information about customers or employees.**
- **Small to medium-sized businesses spent an average of $1.2 million because of damage from cyberattacks in 2019.**

Source: "2019 Global State of Cybersecurity in Small and Medium-Sized Businesses" by Ponemon Institute.

Data Protection Act

INNOVATE Ohio

Mike DeWine, Governor | Jon Husted, Lt. Governor and Director

The Data Protection Act is the first piece of legislation introduced as a result of the CyberOhio Initiative. Senate Bill 220 was signed into law in August 2018 and encourages businesses to voluntarily adopt strong cybersecurity practices to protect consumer data.

The Data Protection Act specifies industry-recognized security frameworks for Ohio businesses to incorporate into their cybersecurity policies. Effective protections save customers from the expense, embarrassment, and harm caused by having their personal information compromised.

The act does not create a minimum cybersecurity standard and is intended to be an incentive for businesses to achieve a higher level of cybersecurity through voluntary action. If a business has a cybersecurity program that meets one of the act's requirements, it is eligible to use that affirmative defense in the event of a lawsuit from the result of a data breach.

Launched in 2016, by then Ohio Attorney General Mike DeWine, the goal of CyberOhio is to help foster a legal, technical, and collaborative cybersecurity environment to help Ohio businesses thrive. In addition to promoting legislation, other parts of the initiative include training opportunities for businesses and development of cybersecurity workforce personnel. CyberOhio is now an InnovateOhio initiative that is led by Lt. Governor Jon Husted.

Affirmative defense

The purpose of the act is to provide an affirmative defense to a lawsuit that alleges a data breach was caused by a business' failure to implement reasonable information- security controls. (An affirmative defense allows a defendant to introduce evidence, that if found credible, can negate civil liability, even if the allegations are true.)

Flexible programs

Under this act, a cybersecurity program is scalable to each business based on:

- Size
- Complexity
- Nature
- Cost
- Resources

Supported security frameworks

The cybersecurity frameworks incorporated into this act:

- National Institute of Standards and Technology (NIST)
- Federal Risk and Authorization Management Program (FedRAMP)
- Center for Internet Security (CIS) Controls
- International Organization for Standardization (ISO) 27000
- Health Insurance Portability and Accountability Act (HIPAA)
- Gramm-Leach-Bliley Act (GLBA)
- Federal Information Security Management Act (FISMA)
- Health Information Technology for Economic and Clinical Health (HITECH) Act
- Payment Card Industry Data Security Standard (PCI DSS)

Contact us at Cyber@Ohio.Gov