Data Protection Act

O.R.C 1354.01 through 1354.05

Formerly Known As "Safe Harbor"

Provides an "Affirmative Defense" to a cause of action sounding in tort related to a data breach which can negate civil liability even if the plaintiff's allegations are true.

Businesses shall Create, Maintain & Comply with a known CyberSecurity program:

1) NIST 800-171
2) NIST 800-53 & 800-53A
3) Center for Internet Security – Critical Security Controls (CIS CSC)
4) ISO/IEC 2700 Family
5) HIPAA
6) GLBA
7) Federal Information Security Modernization (FISMA)

The CyberSecurity program should Protect:

1) against unauthorized access
2) personal information
3) against anticipated threats

Your Business CyberSecurity Scope is based upon:

1) The size & complexity of your business
2) Activities of the business
3) Sensitivity of personal information
4) Cost & Available CyberSecurity tools
5) Resources available to your business

XLN SYSTEMS
614.947.3607
XLNsystems.com

The Process to obtaining Safe Harbor:

1) Choose your program to emulate
    a. Each will contain an effective date
2) Business will have 1 year after said effective date to implement CyberSecurity
    a. During this time period of 1 year, the business is protected by the Safe Harbor statute.
3) If business complies with selected program, it retains its Safe Harbor.

As business owners, you have enough on your plate. Let XLN SYSTEMS lead you through the fog of uncertainty and the magic of technology to guide you to cyber protection.