TANNER

Accountants & Advisors

Right Answers, Right Here.

Utah House Bill 80

Cybersecurity Affirmative Defense Act

House Bill 80

Presentation Overview

- **Current landscape (Privacy Law)**
- **Utah Cybersecurity Defense Act – HB80**
- **Requirements**
- **Frameworks Compared**
- **How do you make the Defense Stick**
- **Questions**

Current Landscape (Privacy Law)

Part 1

Current landscape (Privacy Law)

- CCPA / GDPR
- Nevada – SB 220 / Virginia – SB 1392
- Future of Privacy Legislation

- Problems: Cybersecurity and Data Breach Statutes
  - 50 different state requirements
  - No guidance about how to comply
  - Investment in cybersecurity has counted for little when pursuing breach liability defense
  - Successful legal claims, even when IT controls are set up correctly

Utah Cybersecurity Defense Act

Part 2

Utah Cybersecurity Defense Act – HB80

Key Features

- Incentive to comply (nationally recognized security framework)
- Affirmative defense in a data breach

  - Affirmative Defense:
    - Defense against the claim that an organization failed to implement reasonable controls,
    - Defense against failure to respond to a breach,
    - Defense against failure to appropriately notify individuals

Requirements

Requirements

- ✓ Perform an IT Risk Assessment
- ✓ Create a written cybersecurity program
- ✓ Make sure controls are in place before a breach
- ✓ General Requirements
  - Protect the security, confidentiality, and integrity of personal information
  - Protect against anticipated threats or hazards to security
  - Protect against a breach of system security
- ✓ Framework requirements
  - Conform to one of the frameworks

Requirements - continued

- ✓ Scale & Scope Requirements
  - Consider the size, complexity, nature of activities, cost and availability of tools to improve information
- ✓ Reasonableness Requirement
  - Develop policies, practices and procedures to detect, prevent, and respond to breaches
  - Perform risk assessments on a regular basis

Caution

- The defense doesn't apply if an organization has actual notice of a threat or hazard, failed to act, and the hazard resulted in a breach.
- NOTE: a risk assessment to improve security is not actual notice of a threat or hazard.

Frameworks

Part 3

Frameworks Compared

- NIST 800-171
- NIST 800-53
- FedRamp
- CIS 20
- ISO 27001
- Federal laws for federally protected information (such as HIPAA and GLBA)
- Or PCI-DSS for PCI data

Frameworks

Part 4

How do you make the defense stick

- Choice of law, jurisdiction, and venue clauses in contracts

House Bill 80

Questions ?????