Learning Objectives

- Recognize the pervasiveness of cybercrime;
- Identify the potential costs of experiencing a data breach;
- Understand the best practices that may be implemented to protect a tax preparer from cybercrime
- List the responsibilities of a tax preparer who has experienced a taxpayer data breach.

Chapter 1 – Introduction to Cybercrime

- The Nature of Cybercrime
- Phishing
- Staying Current on Cyberthreats & Avoidance Strategies
- FBI Internet Crime Report

Chapter 2 – Laws & Regulations Safeguarding Taxpayer Data

- The Gramm-Leach-Bliley Financial Modernization Act
- Sarbanes-Oxley Act of 2002
- Penalties for Unauthorized Disclosure or Use of Taxpayer Information

Chapter 3 – The Costs of a Data Breach

- Data Breach
- Cybercrime Costs
- Probability of Experiencing a Data Breach

Chapter 4 – The Information Security Plan

- Ensuring Data Security
- Where to Begin: Determining Responsibility
- Identifying the Risks and Their Impact
- Writing an Information Security Plan

Chapter 5 – Best Practices for Securing Data

- Recommended Practices
- Maintaining Information System Security

Chapter 6 – When a Data Breach Occurs

- When a Data Breach Occurs
- Secure the Firm's Operations
- Remove Improperly Posted Information from the Web
- Interview
- Fix Vulnerabilities
- The Firm's Communications Plan
- Notify Appropriate Parties