WISP
Written Information Security Plan

technology associates

Agenda

- Introduction
- Overview of WISPs
- WISPs and CPAs
- The Main Thing
- Elements of a WISP
- 314.6 Exceptions [*maybe*]
- Notifications
- Best Practices
- Resources
- Conclusion

Introduction

- I.T. industry since 1991, consulting since 1997
- Work with CPA firms across state for over 25 years
- CISSP - Certified Information Systems Security Professional
  - International Information System Security Certification Consortium - ISC2
- CISM - Certified Information Security Manager
  - Information Systems Audit and Control Association - ISACA
- Over 60 hours of research on this topic
- I.T. w/o the B.S.

Overview of WISPs

- Gramm-Leach-Bliley Act (GLBA)
- FTCs “Safeguards Rule”
  - Title 16 Code of Federal Regulations Part 314
  - Standards for Safeguarding Customer Information
- Safeguards Rule
  - December 2021
  - Last Updated May 2024 (notification events)

Overview of WISPs (cont.)

- "Financial Institutions" under GLBA/Safeguards
  - Tax and accounting professionals are considered financial institutions, regardless of size or number of clients
- Safeguards Rule Requires a WISP
  - Written Information Security Plan (WISP)
  - Written and accessible [offsite]
  - W-12 Requirement since 2019

11 Data Security Responsibilities	I am aware that paid tax return preparers are required by law to create and maintain a written information security plan that provides data and system security protections for all taxpayer information. ☐ See IRS Publication 5708 and 4557 for more information about your responsibilities.

Form **W-12** (Rev. 10-2024)

WISPs and CPAs

- IRS Publication 5708 (August 2024)
  - IRS & Security Summit
  - Year-long effort
  - Aimed at helping Tax Pros implement WISPs
  - “Sample Information”
  - “..not intended to replace your own research, to create reliance or serve as a substitute for developing your own plan based upon the specific needs and requirements of your business or firm.”

Keep The Main Thing The Main Thing!

- Protecting Customer Information
- ***Customer information*** means any record containing nonpublic personal information about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of you or your affiliates. 16 CFR 314(d)
- Focus on the Data

Elements of a WISP

- Designate a Qualified Individual
- Conduct a Risk Assessment
- Design and Implement Safeguards
- Regularly Monitor and Test
- Train Your Staff
- Monitor Your Service Providers
- Keep Your Program Current
- Create an Incident Response Plan
- Require Annual Report

Elements of a WISP

- Designate a Qualified Individual
  - QUALIFIED!
  - Responsible for implementing / enforcing WISP
  - Can be an employee or an affiliate
  - If not an employee;
    - YOU are still ultimately responsible
    - You must designate a ‘senior’ member of your staff for direction and oversight
    - Require your service provider to maintain WISP

Elements of a WISP

- Conduct a Risk Assessment [*maybe*]
  - Complete inventory
  - Highlight Customer Information (PII)
  - CIA Triad (Confidentiality / Integrity / Availability)
  - *DAD Triad (Disclosure / Alteration / Destruction)*
  - Assess Likelihood / Impact
  - Threat Modeling
  - Must be in writing [*maybe*]
  - ‘Periodically’ refresh

Elements of a WISP

- Design and Implement Safeguards
  - Based on Risk Assessment [*maybe*]
  - Requirements from 16 CFR 314
    - Review access controls
    - Identify & manage data, personnel, devices, systems
    - **Encrypt Customer Information**
    - ~~Adopt Secure Development Practices~~
    - Implement Multi-Factor
    - Dispose of Customer Info Securely (COD)
    - Adopt Change Management Process
    - Log User Activity

Elements of a WISP

- Regularly Monitor and Test [*maybe*]
  - Continuous monitoring
  - Annual Penetration Testing
  - Vulnerability Scans Every 6-months

Elements of a WISP

- Train Your Staff
  - Trained on your policies and procedures
  - Security Awareness Training
  - Utilize “qualified information security personnel employed by you, or an affiliate or service provider” 16 CFR 314
  - If employed; “Providing information security personnel with security updates and training sufficient to address relevant security risks”
  - If Outsourced: “Verifying that key information security personnel take steps to maintain current knowledge of changing information security threats and countermeasures”

Elements of a WISP

- Monitor Your Service Providers
  - (f) Oversee service providers, by:
    - (1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue;
    - (2) Requiring your service providers by contract to implement and maintain such safeguards; and
    - (3) Periodically assessing your service providers based on the risk they present and the continued adequacy of their safeguards.

Elements of a WISP

- Keep Your Program Current
  - Changes to operations (mergers/acquisitions)
  - Changes to systems (migrations)
  - Changes to personnel
  - Changes in emerging threats
  - Annually
    - Review / Update Risk Assessment
    - Review / Update WISP
    - Review Service Provider

Elements of a WISP

- Create an Incident Response Plan [*maybe*]
  - Prompt Respond and Recovery from security event
  - Should Include;
    - The goals of the plan
    - The internal processes for responding to a security event
    - The definition of clear roles and responsibilities
    - External and internal communications
    - Remediation requirements of any identified weaknesses
    - Documentation and reporting regarding security events
    - The evaluation / revision of incident response plan

Elements of a WISP

- Require Annual Report [*maybe*]
  - "Qualified individual" must report in writing at least annually
  - To Board or 'senior officer'
  - Report on status of WISP and compliance with 314.4
  - And "Material matters related to the information security program, addressing issues such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security events or violations and management's responses thereto, and recommendations for changes in the information security program."

314.6 Exceptions

- [86 FR 70308, Dec. 9, 2021]
- 314.6 exempted financial institutions that maintain customer information concerning fewer than five thousand consumers from certain requirements of the Proposed Rule, namely
  - § 314.4(b)(1), requiring a written risk assessment
  - § 314.4(d)(2), requiring continuous monitoring or annual penetration testing and biannual vulnerability assessment
  - § 314.4(h), requiring a written incident response plan
  - § 314.4(i), requiring an annual written report by the CISO (as revised, the Qualified Individual)
- This proposed section was designed to reduce the burden on smaller financial institutions.

Notifications

- Federal - FTC
  - If > 500 un-encrypted records are exposed
  - Within 30-days of discovery
  - No law enforcement delay
  - There is a form for that…

  - “The Commission also agrees notification should not be required when harm to consumers is rendered extremely unlikely because the customer information is encrypted”

Notifications (cont.)

- IRS
  - Stakeholder Liaison
- Federal - FBI
  - If cyber-crime
  - Internet Crime Complaint Center (IC3)
- Business Partners
  - Attorney
  - Tax Software Vendor
  - Cyber-Liability Carrier?

Notifications (cont.)

- NC State
  - G.S. 75-67
  - "…shall notify the owner or licensee of the information of any security breach immediately following discovery of the breach…"
  - "In the event a business provides notice to an affected person pursuant to this section, the business shall notify without unreasonable delay the Consumer Protection Division of the Attorney General's Office of the nature of the breach, the number of consumers affected by the breach, steps taken to investigate the breach, steps taken to prevent a similar breach in the future, and information regarding the timing, distribution, and content of the notice."
  - Law enforcement delay - in writing
  - If > 1,000, must notify all consumer reporting agencies

Best Practices

- Shrink your foot-print / exposure
  - Data – locations / retention
  - Access – only to those that MUST have access
- Encryption / Multi-Factor
- Regular review and updates
- Outsourcing doesn't outsource the responsibility!
- Have attorney review incident response plan
- Time Annual Report just after
  - Annual risk assessment review
  - Annual Pen-test
  - Annual Service Provider Review

Resources

Thank you!

Further Questions?

Eric Hobbs
ehobbs@technologyassociates.net
https://www.linkedin.com/in/hobbseric/