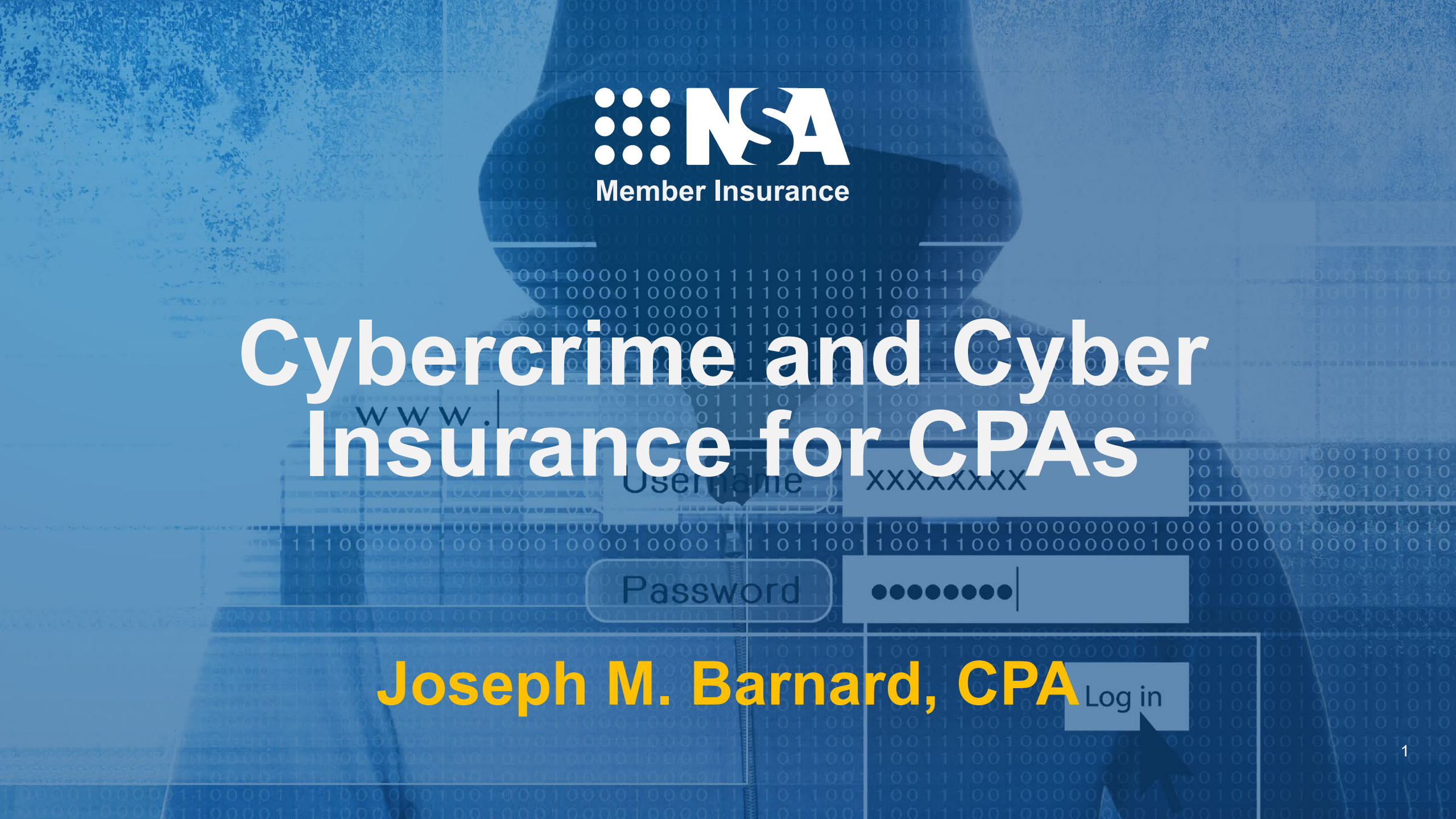
NSA
Member Insurance
Cybercrime and Cyber Insurance for CPAs
Joseph M. Barnard, CPA
Log in

Agenda

- Cybercrime and Statistics
- Professional Obligations
- Cyber Insurance Policies
- What to Do During a Cyber Incident
- Avoiding Cyber Insurance Exclusions

Treasury Department / IRS

Treasury Department Circular No. 230 (Rev. 6-2014)

- § 10.52 Violations subject to sanction.
- (a) A practitioner may be sanctioned under §10.50 if the practitioner —
  - ✓(1) Willfully violates any of the regulations
  - ✓(2) Failing to adhere to the circular (**recklessly** or through **gross incompetence)**

Requirement added to Form W-12, IRS Paid Preparer Tax Identification Number (PTIN) Application (Rev. 10-2023)

11	**Data Security Responsibilities**	I am aware that paid tax return preparers must have a data security plan to provide data and system security protections for all taxpayer information. ☐

Form **W-12** (Rev. 10-2023)

Gramm-Leach-Bliley (GLB) Act of 1999

GLB gives the Federal Trade Commission (FTC) authority to regulate information safeguard protocols for businesses that are "significantly engaged" in providing financial products or services, including professional tax preparers.

- Safeguards Rule: requires companies to develop a written information security plan (WISP) stating the company's policies and procedures for protecting customer information
- WISP must be tailored based on company's size and activities, and the complexity and sensitivity of customer information

Key Elements of a Data Security Plan*

Element	Description
 **Coordination**	Designate one or more employees to coordinate the information security program
 **Risk Identification**	Identify and assess risks to customer information in each relevant area of the company's operation
 **Effectiveness of Safeguards**	Evaluate the effectiveness of current safeguards to control the risks
 **Service Provider Selection**	Select service providers that can maintain appropriate safeguards
 **Contractual Obligations**	Ensure your contract requires service providers to maintain safeguards
 **Service Provider Oversight**	Oversee service providers' handling of customer information
 **Continuous Improvements**	Evaluate and adjust the program to adapt to changes in the firm's business or operations, or results of testing and monitoring
 **Elements from Key Checklist Areas**	Specific requirements on employee training and management, information systems, and detecting and managing system failures

*IRS Publication 4557, Safeguarding Taxpayer Data

Cyber breaches of CPA firms*

Reported data breaches of CPA firms have increased by over **80%** since 2014

- The portion of breaches that include **ransomware extortion** has risen to **over 40%** since 2018

CPA Firm Incident-Related Expense	Estimated Costs
Forensic discovery, remediation, reporting, and outside counsel	**$70K-$300K**
State and federal reporting and credit monitoring requirements	**$100K-$300K**
Ransom Amounts Note: Paying the ransom does not guarantee the systems will be recoverable	**$100K** for a small firm to **$2.6 million** for a large firm
Reputational Costs	Not included

*The Tax Advisor, April 1, 2020

Cyber Insurance: Coverage Structure

1st Party
Breach Response
Business Interruption
Cyber Extortion

3rd Party
Network & Information
Security Liability
Regulatory Defense & Penalties
Technology & Media Liability

Key Considerations for Cyber Insurance Coverage:

- Does the policy offer full prior acts coverage?
- Does the policy pay on behalf of the insured, or does it reimburse?
- Are sublimits of liability associated with higher risk events (cybercrime, extortion, transfer fraud) reduced / acceptable?
- Loss of income: Is this a defined term, and is there a stated methodology to determine the amount of loss?

Incident and Breach Response

Reporting Incident to the Insurance Company

- Condition for coverage – report immediately
- Company will send reservation of rights letter confirming reporting

Insurance Company Assigns Breach Coach (Attorney)

- Breach coach assigns outside vendors to determine key incident facts and perform coordinated response

Rapid Coordinated Response by Specialized Trained Professionals

- Forensics determine key incident facts (what/who was impacted, when incident happened)
- Notification statutory language as required by each state
- Credit monitoring for victims

Avoiding Common Cyber Claim Denials

Accuracy of affirmative statements made in the cyber policy application:

- Enforcement of multi-factor authentication (MFA), encryption, patch management, backups, email filtering, and computer (endpoint) protection
- Prior knowledge of potential claims – 3rd Party
- Funds transfers – secondary means of communication validating authenticity

Recommendation: Have your IT personnel / IT service review cyber policy application for accuracy prior to purchase.

Notable Policy Exclusions

The worst time to analyze your policy is after a claim has been made!

- Retroactive date – be aware of this significant date
- Prior knowledge – both knowledge and previous reporting to other carriers
- War and terrorism – should exclude (cover) cyber terrorism.

Recommendation: Request full prior acts due to the short tail nature of cyber claims.

Recommendations

Buy Cyber Insurance

- Request full prior acts coverage
- IT personnel / IT vendor reviews application for accuracy
- Review your policy for terms and conditions – don't wait until a claim has been made!

Questions?

Contact Joe Barnard at jbarnard@ftj.com