CYBERPROTECT
OVERVIEW

CPA Mutual®
INSURANCE COMPANY OF AMERICA
RISK RETENTION GROUP
Providing Services to CPAs by CPAs Since 1987

As more information is stored and shared online, in email, and on mobile devices, there is greater risk of theft or exposure of that information by cyber criminals. Cyber criminals are smart and opportunistic. They look for the quickest way to get in, get information, and get out without being detected, and they seem to always be one step ahead. In recent years, cyber criminals have increasingly targeted small businesses and CPA firms. In fact, you may have already been the target of a cyber criminal without knowing it.

Is YOUR firm cyber safe?

CPA Firms Under Attack

- Cyber breaches hit a record high in 2017 - a 45% increase over 2016.[1]
- Small to midsize businesses in the financial industry saw a substantial uptick in email malware, increasing by nearly 50% in 2016.[2]
- In 2016, businesses with less than 250 employees were the biggest targets of phishing email scams, such as a false funds transfer request.[3]

Cyber Security Tips

- Train employees in security principles
- Protect data, computers and networks from cyber-attacks
- Install network firewall protection
- Create a mobile device action plan
- Make backup copies of important business data and information
- Control physical access to your computers and create user accounts for each employee
- Secure your Wi-Fi networks
- Comply with the Payment Card Industry Data Security Standard guidelines if you accept credit or debit card payments
- Limit employee access to data and information; limit authority to install software
- Require passwords and authentication

Risk Management

Being insured isn't the same as being prepared. Your accountants professional liability insurance includes access to online cyber risk management resources and tools to help you identify and mitigate cyber risks. You'll have access to:

- Privacy materials to help you analyze and adhere to state and federal compliance laws
- Online training and support including best practices for password safety and defense against ransomware
- Training courses and webinars to generate cyber risk awareness among management and employees
- Guidance for setting up a breach response plan to react quickly and effectively.

Breach Response Services

If you have a breach, expert claims examiners coordinate the breach response team and assist you throughout the process until the claim is resolved.

Our assigned legal counsel acts as your "breach coach" - the point person who will coordinate all breach response activities. If necessary, specialists may be engaged, including:

- IT security and forensic experts
- Public relations/advertising support
- Breach notification
- Call center and website support
- Credit monitoring and identity theft restoration services

Sources: 1. www.idtheftcenter.org, 2017 Annual Data Breach Year End Review | 2-3. www.symantec.com, Symantec Internet Security Threat Report, Volume 22

CYBERPROTECT COVERAGE

CPA Mutual® INSURANCE COMPANY OF AMERICA RISK RETENTION GROUP
Providing Services to CPAs by CPAs Since 1987

First Party Losses

Privacy Breach Response Costs, Notification Expenses and Customer Support and Credit Monitoring Expenses- Coverage for mitigation costs and expenses incurred because of a privacy breach, security breach or adverse media report, including legal expenses, public relations expenses, IT forensic expenses, and costs to provide credit monitoring and identity theft assistance to affected individuals. Includes:

- **Proactive Privacy Breach Response Costs-** Coverage for public relations expenses incurred in response to a security breach or privacy breach, but prior to the publication of an adverse media report.

- **Voluntary Customer Notification Expenses-** Coverage for expenses incurred in notifying parties of a privacy breach where there is no requirement by law to do so.

Network Asset Protection- Coverage for income loss, interruption expenses, and data recovery costs incurred due to a variety of causes, from accidental damage of electronic media to cyber attacks that cause a total or partial interruption of an insured computer system.

Cyber Extortion- Coverage for extortion expenses incurred and extortion monies paid as a direct result of a credible cyber extortion threat.

Cyber Terrorism- Coverage for loss of business income and interruption expenses incurred as a direct result of a total or partial interruption of an insured computer system due to an act of cyber terrorism.

BrandGuard®- Coverage for loss of revenue incurred as a direct result of an adverse media report or notification to affected individuals following a security breach or privacy breach.

Third Party Claims

Multimedia Liability- Coverage for third party claims alleging liability resulting from the dissemination of online or offline media material, including claims alleging copyright/trademark infringement, libel/slander, plagiarism, or personal injury.

Security & Privacy Liability- Coverage for third party claims alleging liability resulting from a security breach or privacy breach, including failure to safeguard electronic or non-electronic confidential information, or failure to prevent virus attacks, denial of service attacks or the transmission of malicious code from an insured computer system to the computer system of a third party.

Privacy Regulatory Defense and Penalties- Coverage for regulatory fines and penalties and regulatory compensatory awards incurred in privacy regulatory proceedings/investigations brought by federal, state, or local governmental agencies.

PCI DSS Assessments- Coverage for assessments, fines, or penalties imposed by banks or credit card companies due to non-compliance with the Payment Card Industry Data Security Standard (PCI DSS) or payment card company rules.

CYBERPROTECT
RISK SCENARIOS

CPA Mutual®
INSURANCE COMPANY OF AMERICA
RISK RETENTION GROUP
Providing Services to CPAs by CPAs Since 1987

Privacy Breach Response Costs, Notification Expenses, and Customer Support and Credit Monitoring Expenses Coverage

A programming error within the computer system at a CPA firm allowed client information to become publicly visible on the internet. Approximately 8,700 clients were affected by the breach. Cyber insurance paid for breach response costs, including breach notification costs, IT forensic expenses, legal fees, and public relations expenses, all totaling more than $125,000.

Cyber Extortion Coverage

A hacker seized control of a CPA firm's computer system using malware which infected the firm's computers and network. The hacker demanded a ransom of 40 bitcoin, the equivalent of $370,000, to give the firm back control of its systems. Cyber insurance covered the ransom payment.

Security and Privacy Liability Coverage

An accountant prepared a tax return for a client, and her office manager emailed the return to the client. A few days later, the client called for an update on the status of her tax return, stating she never received the officer manager's email. It was then discovered that the officer manager had inadvertently sent documents, containing personally identifiable information, to the wrong email address. The client filed a lawsuit against the accountant for negligence and failure to safeguard confidential information. Cyber insurance paid for the costs to defend the lawsuit and covered damages.

PCI DSS Assessment Coverage

A tax preparer office accepts credit and debit card payments from customers. The tax preparer was notified by a credit card company that several of its customers had reported fraudulent credit card purchases, and the credit card company's investigation revealed that the security breach originated from tax preparer's point of sale system. The investigation further concluded that tax preparer did not have the required security controls in place to protect card data and subsequently issued fines against the tax preparer for failure to comply with Payment Card Industry Data Security Standard guidelines. Cyber insurance paid for the fines levied by the credit card company.