CYBER RISK EXPOSURE SNAPSHOT

# Your CPA-Ready Annualized Risk Cost Summary

**Unmanaged Exposure**

ANNUALIZED CYBER RISK COST

## $79K - $242K / year

Your responses suggest material exposure that should be prioritized and reduced before an incident forces the issue.

This dollar figure is an **annualized expected risk-cost range**: likelihood multiplied by estimated impact. It is not a prediction of what one incident will cost, and it does not determine whether the organization is secure or compliant.

Mode: Full Advisory Assessment | Model: 2026.06-v5.15-scroll-to-question | Vertical: Financial services / fintech / wealth management

Potential oversight drivers selected: NYDFS or state financial services rules, State privacy or breach notification laws

## If the top scenario occurs

RANSOMWARE & SYSTEM SHUTDOWN

## $342K - $788K

This is the estimated impact range for the top scenario if it occurs. The annualized risk-cost figure above is probability-weighted.

## Next best action

**Validate backup restoration and incident response readiness.**

Backup uncertainty and unclear response ownership can increase downtime, recovery costs, and insurance friction.

## Estimate confidence

**High Confidence**

Most key inputs were answered directly, so the estimate is more supportable as a planning range.

**Score:** 95/100

## Compliance & Evidence Readiness

**Documentation Gap Identified**

The organization may have meaningful documentation and evidence gaps that should be addressed before an incident, insurer request, client review, or regulatory inquiry.

**Score:** 2/12

## CPA Client Conversation Summary

Based on the responses, the most important cyber risk conversation is **WISP, evidence folder, insurance support, and compliance roadmap**.

The client's exposure appears to be driven by **Ransomware & System Shutdown**. This is not only a technical issue. It is a financial exposure, documentation, insurance, internal control, and client trust conversation.

**What this may affect:**

- Payroll and benefit processing
- Billing, collections, and cash flow
- Financial reporting and close process
- Tax, filing, or client-service deadlines
- Management time and recovery costs

## Top attack scenario

**Ransomware & System Shutdown**

Downtime, backup recoverability, and incident response readiness

**Fastest next step:** Test backup restoration and create a one-page incident response plan.

## Advisory opportunity

**WISP, evidence folder, insurance support, and compliance roadmap**

Use this as the bridge from cyber risk to financial impact, internal controls, documentation, insurance, and reasonable next steps.

## Evidence to validate next

A good follow-up engagement should validate assumptions before prescribing solutions.

- Most recent successful backup restore test
- Backup scope and retention documentation

- Incident response call tree
- Cyber insurance downtime assumptions

## Why this matters to a CPA

If policies, practices, and evidence do not align, the organization may struggle to support insurance applications, client security requests, breach response, or regulatory expectations.

## Scenario Breakdown

### Ransomware & System Shutdown

Downtime, backup recoverability, and incident response readiness

**$43K-$99K**

**Recommended action:** Test backup restoration and create a one-page incident response plan.

### Sensitive Data Exposure

Sensitive client, customer, patient, employee, or financial records

**$12K-$91K**

**Recommended action:** Identify sensitive data, restrict access, and align WISP and documentation with actual practices.

### Vendor / Payroll / IT Provider Incident

Third-party dependency and operational disruption from vendors

**$18K-$40K**

**Recommended action:** Review vendor access, contracts, breach notice terms, and continuity assumptions.

### Email & Payment Fraud

Email compromise, payment-change procedures, and transfer exposure

**$6K-$10K**

**Recommended action:** Require out-of-band payment verification and MFA for email and banking.

### AI / Shadow Data Risk

Use of AI tools with company, client, or sensitive data

**$0-$2K**

**Recommended action:** Publish AI usage guidance and prohibit sensitive data in unapproved tools.

## How this estimate was calculated

Annualized Risk Cost = Scenario Likelihood x Scenario Impact. The dollar figure is an annualized expected cost range, not a prediction of a single incident cost. Revenue informs downtime exposure. Payment size informs fraud exposure. Sensitive records inform data exposure. Vertical and controls modify likelihood and impact. Insurance review modifies

retained exposure. "Not sure" answers reduce confidence.

## Potential Cyber Compliance Drivers

| Potential driver | Why it may matter |
|---|---|
| **FTC Safeguards / GLBA** | Written security program, risk assessment, safeguards, vendor oversight, monitoring, and incident response may be relevant. |
| **Financial services cybersecurity rules** | Risk assessment, access controls, incident response, vendor oversight, and governance evidence may be relevant. |
| **State privacy or breach notification laws** | Notification timing, affected resident analysis, recordkeeping, legal review, and response documentation may be relevant. |
| **Cyber insurance requirements** | Applications, control representations, MFA, backup testing, incident response, and claim documentation may be relevant. |

This map identifies potential drivers to review. It does not determine legal applicability.

## Policy / Practice / Proof gaps

CPAs can use these gaps to frame the next conversation around evidence, not technical jargon. The goal is not perfection. The goal is to show that the organization understood risk, made reasonable decisions, implemented safeguards, and can document what it did.

- Written security program / WISP
- Documented risk assessment
- Evidence folder readiness

## Questions a CPA can ask next

- How long could payroll, billing, collections, and reporting continue if key systems were unavailable?
- What stops first if email, file access, or the accounting system goes down?
- When was the last successful backup restore test?
- Who has authority to make decisions during a cyber incident?
- Who owns cyber risk at the executive or management level?
- Could the organization produce supporting cybersecurity documentation within 48 hours?
- What evidence supports the organization’s cyber insurance application answers?

## Evidence folder checklist

These are the types of materials a firm or client should be able to locate before an insurer, regulator, client, or incident response event forces the issue.

- Current Written Information Security Program or written cybersecurity plan
- Documented cyber risk assessment
- MFA implementation evidence

- Backup restore test record
- Incident response plan and call tree
- Employee security training records
- Vendor oversight documentation
- Cyber insurance application support
- Payment-change verification procedure
- AI usage policy or approved-tools guidance

## Suggested 90-Day Action Plan

### First 30 days

- Identify systems that support payroll, billing, collections, reporting, and client service.
- Confirm backup ownership, backup location, and last successful restore test.
- Define who gets called first during an incident.

### Days 31-60

- Test backup restoration and document the result.
- Create or update a one-page incident response checklist.
- Review cyber insurance against realistic downtime assumptions.

### Days 61-90

- Conduct a tabletop exercise.
- Update the written security program and evidence folder.
- Review business continuity assumptions with leadership.

## Use this with a client or internal stakeholder

Start with this softer follow-up email. To save the full summary, use the print button and choose “Save as PDF.”

- Who has authority to make decisions during a cyber incident?

Suggested next validation step:
Validate backup restoration and incident response readiness.

This may be useful for our next check-in because it connects cyber risk to continuity, fraud controls, documentation, insurance, and management decision-making.

Best,
Saul

## Use this result

Start with the checklist, review the scenario with the right people, or validate the assumptions behind the number.

### 1. Get the checklist

Send me the Backup & Continuity Checklist

### 2. Review the scenario

Validate Backup & Business Continuity Assumptions

### 3. Validate assumptions

Review backup restore evidence, recovery expectations, incident response ownership, and business interruption assumptions.

Review the assumptions behind the risk-cost estimate and identify the most practical exposure-reduction steps.

opinion, technical audit, insurance determination, or guarantee of security.

### What does the dollar amount mean?

Quickly and efficiently build the materials you need to support your inbound marketing strategy. Drag and drop building blocks including testimonials, forms, calls-to-action, and more.

### Is this a compliance determination?

No. The tool identifies potential compliance and evidence-readiness considerations. Applicability should be reviewed with appropriate legal, insurance, or regulatory advisors.

### Is this a technical audit?

No. It is a business-risk screening tool designed to identify scenarios worth validating.