Cybersecurity for CPAs: What You Need to Know

CPA Ontario Centre in Digital Financial Information

Andrea Seaton Kelton, PhD
MTSU Accounting Advisory Board Outstanding Professor
Professor of Accounting
Middle Tennessee State University

Agenda

WHY SHOULD CPAS CARE ABOUT CYBERSECURITY?

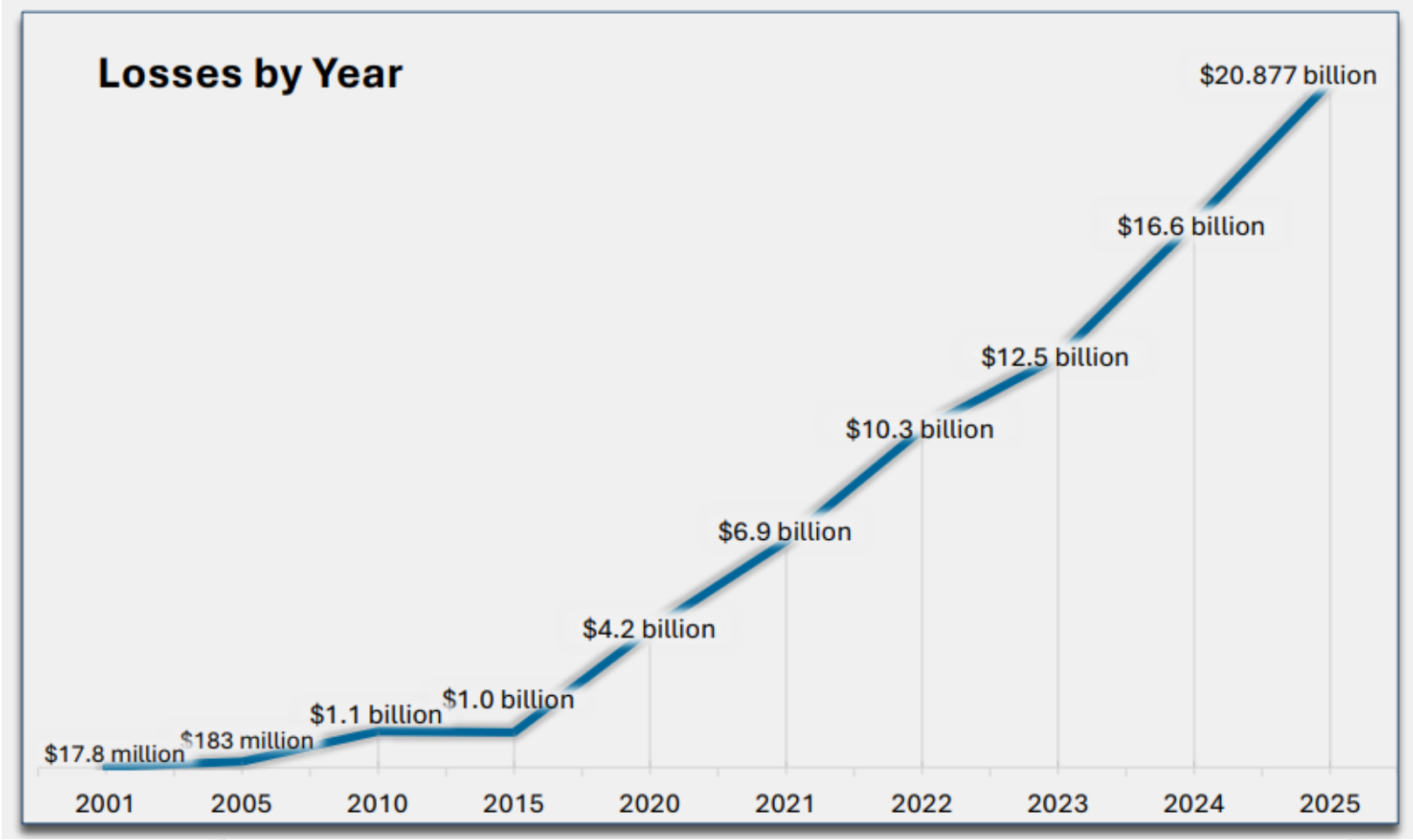
HOW CAN WE PROTECT OURSELVES?

HOW CAN WE HELP OUR CLIENTS?

Why should CPAs care about cybersecurity?

Cybersecurity threats are increasing

Cybercrime has become highly profitable

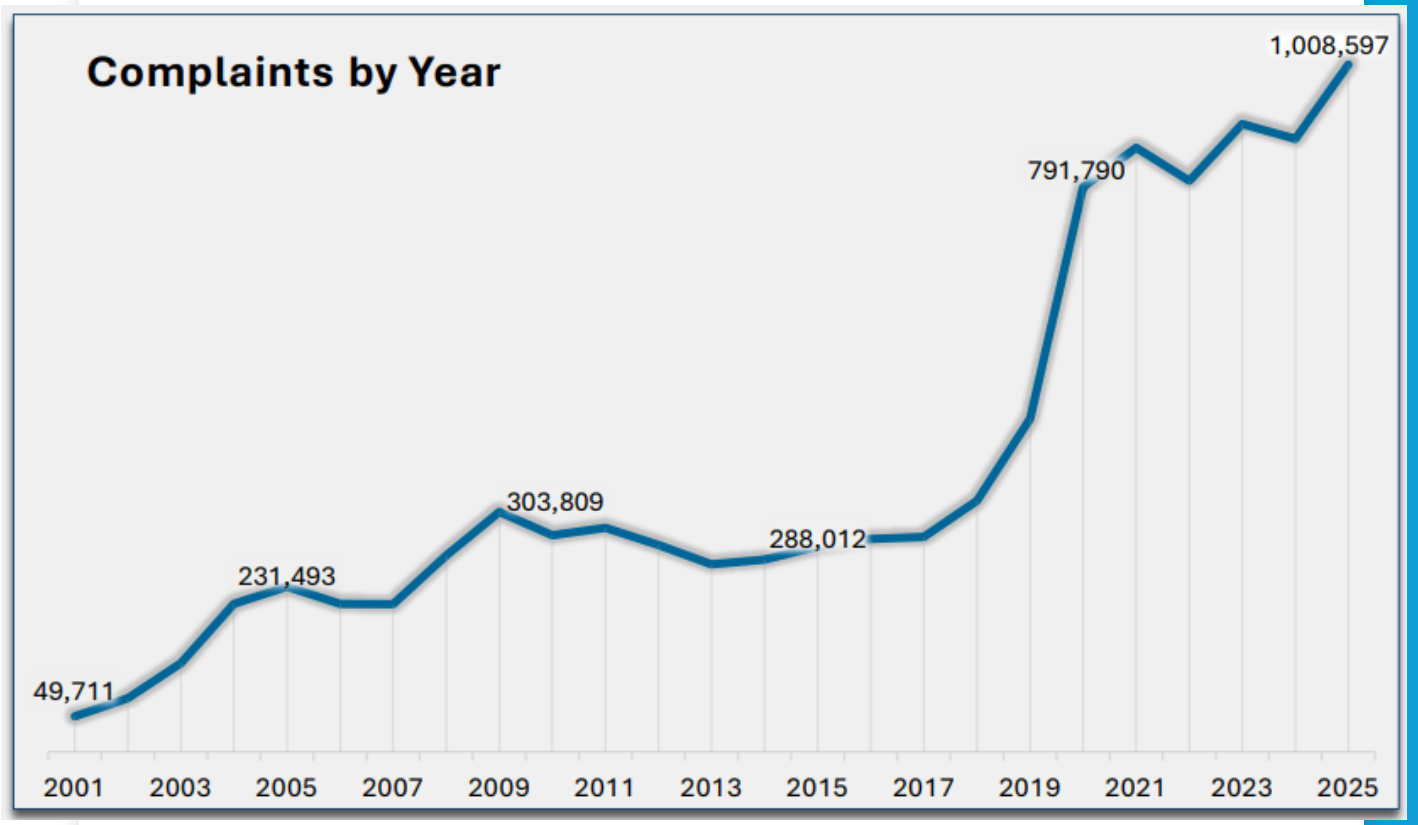


Source

Cybersecurity threats are increasing

Greater opportunity for attacks:

- Explosion of digital data
- Increased reliance on cloud systems and remote work



Source

Cybersecurity breaches are costly

(IBM 2025)

In 2024, the global average cost of a data breach was USD 4.44 million

- In the US, the average cost was USD 10.22 million
- In Canada, the average cost was USD 4.84 million

65% of organizations have not fully recovered from a breach

Cybersecurity breaches impact the entire industry – contagion effects

Cyber criminals are getting smarter and faster

(CrowdStrike 2026)

AI-enabled attacks increased by 89% – mainly through AI-generated phishing and deepfake impersonation attacks (CrowdStrike 2026)

The average eCrime breakout time was 29 minutes, down from 48 minutes in 2024 (CrowdStrike 2026)

82% of attacks were malware-free, making them harder to detect

Many cyber incidents are governance failures, not IT issues

(IBM 2025)

The average time to identify and contain a breach was 241 days

26% of breaches occurred due to human error

63% of breached organizations do not have a formal AI governance policy

Cybersecurity is a trust and liability issue for CPAs

Litt et al. (2023)

- In 2017, Deloitte suffered a cybersecurity breach
- For 6 months, hackers had access to client emails and username, passwords and IP addresses and other sensitive business information
- As a result of the breach:
  - Existing clients were **no more likely to dismiss Deloitte** post breach
  - Audit clients and existing shareholders became **less likely to approve of Deloitte as the company's auditor.**
  - Deloitte's **audit clients suffered significant negative market** reactions post breach

Cybersecurity is a trust and liability issue for CPAs

(Alhusaini et al. 2025)

Studied 868 IPOs audited by Big 4 firms from 2005–2018.

When an auditor had experienced a **data breach before an IPO**, companies ended up **lowering their IPO price revisions by about 4.1%.**

That translates to roughly **$8.9 million in lost capital per IPO on average** in this sample.

The results suggest that **auditor data breaches damage reputation**, because investors perceive **higher information risk—**even when the financial statements themselves may be unchanged.


Cybersecurity is no longer just
an IT problem.

How can CPAs protect themselves from cyber attacks?


CPAs are high-value targets
for cyber attacks

A BEC EXAMPLE

- Fraudster compromises legitimate email accounts through social engineering or other methods

- In 2025, IC3 received over 24,000 complaints with losses over $3 billion

---------- Forwarded message ---------
From: **Tim Holmes** <tim@holmesswaffordcpa.com>
Date: Fri, Mar 29, 2024, 5:51 PM
Subject: Urgent Notice: Tax Refund
To: laura@holmesswafford.com <laura@holmesswafford.com>

Good evening,

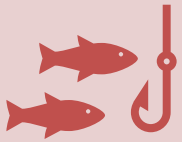
I have just received an important notice from IRS regarding your tax return, apologies for the late response.
It's important I reach out to you before the end of the day.
I'll be working from home to get this resolved.
Laura will also be working from home so you can reach back to either of us. We'll be looking forward to your email response.

Please acknowledge email receipt.

Best regards,

Tim Holmes
HOLMES & SWAFFORD CPAs
820 N. Thompson Lane, Suite 1E
Murfreesboro, TN 37129-4340
Phone 615.295.2782 Direct 615-869-7965

What are the most common cyber threats for CPAs?



Phishing or spear fishing

Ransomware attacks

Third-party risks

Why are humans the “weakest link”

Highly susceptible to social engineering tactics

High pressure periods increase vulnerability

Common behavioral risks:

Password reuse

Clicking unknown links

Rushing approvals

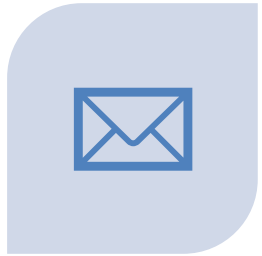
Core Cyber Hygiene Practices to Protect Your Firm From Cyber Attacks

STRONG PASSWORD POLICIES & PASSWORD MANAGERS

MULTI-FACTOR AUTHENTICATION EVERYWHERE POSSIBLE

REPORTING CHANNELS FOR CYBER ATTACK ATTEMPTS

DEVICE SECURITY: UPDATES, ENCRYPTION, SCREEN LOCKS



SAFE FILE SHARING AND EMAIL ATTACHMENT PRACTICES

CYBERSECURITY INSURANCE

Training & Education - *Trust, but verify*

Ongoing (not one-time) cybersecurity awareness training

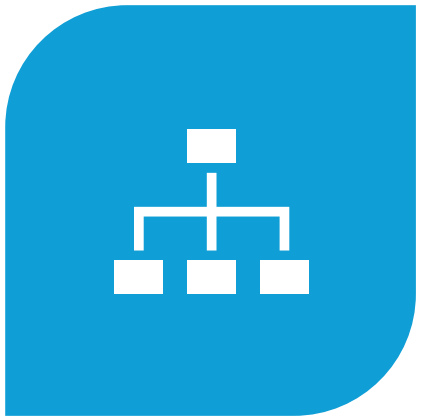
Phishing simulation exercises

How can CPAs help their clients with cybersecurity?

Help our clients manage their cyber risks

HELP CLIENTS IDENTIFY WHERE THEY ARE MOST EXPOSED TO RISK

HELP CLIENTS STRENGTHEN BASIC INTERNAL CONTROLS



ADDRESS THIRD-PARTY AND VENDOR RISKS – SYSTEM AND ORGANIZATION CONTROLS (SOC) REPORTS

Help our clients with their cyber disclosures

“Today, cybersecurity is an emerging risk with which public issuers increasingly must contend. Investors want to know more about how issuers are managing those growing risks… I think companies and investors alike would benefit if this information were required in a consistent, comparable, and decision-useful manner.”

— former SEC Chair Gary Gensler, March 2022

US Disclosure Rules

- In 2023, the US SEC issued new disclosure requirements for cybersecurity risk and breach disclosure

- Disclosure of material cybersecurity incidents **within 4 business days in item 1.05 of form 8-K**

- Describe material aspects of the incident with respect to its: **nature, timing, scope and impact**

Example Disclosures

Item 1.05. Material Cybersecurity Incidents

On January 12, 2024, Microsoft (the "Company" or "we") detected that beginning in late November 2023 a nation-state associated threat actor had gained access to and exfiltrated information from a very small percentage of employee email accounts including members of our senior leadership team and employees in our cybersecurity, legal, and other functions, on the basis of preliminary analysis. We were able to remove the threat actor's access to the email accounts on or about January 13, 2024. We are examining the information accessed to determine the impact of the incident. We also continue to investigate the extent of the incident. We have notified and are working with law enforcement. We are also notifying relevant regulatory authorities with respect to unauthorized access to personal information. As of the date of this filing, the incident has not had a material impact on the Company's operations. The Company has not yet determined whether the incident is reasonably likely to materially impact the Company's financial condition or results of operations.

Example Disclosures

Item 1.05 Material Cybersecurity Incident.

On May 11, 2025, Coinbase, Inc., a subsidiary of Coinbase Global, Inc. ("Coinbase" or the "Company"), received an email communication from an unknown threat actor claiming to have obtained information about certain Coinbase customer accounts, as well as internal Coinbase documentation, including materials relating to customer-service and account-management systems. The communication demanded money in exchange for not publicly disclosing the information. The threat actor appears to have obtained this information by paying multiple contractors or employees working in support roles outside the United States to collect information from internal Coinbase systems to which they had access in order to perform their job responsibilities. These instances of such personnel accessing data without business need were independently detected by the Company's security monitoring in the previous months. Upon discovery, the Company had immediately terminated the personnel involved and also implemented heightened fraud-monitoring protections and warned customers whose information was potentially accessed in order to prevent misuse of any compromised information. Since receipt of the email, the Company has assessed the email to be credible, and has concluded that these prior instances of improper data access were part of a single campaign (the "Incident") that succeeded in taking data from internal systems. The Company has not paid the threat actor's demand and is cooperating with law enforcement in the investigation of this Incident.

The Incident did not involve the compromise of passwords or private keys, and at no time were any of the targeted contractors or employees able to access customer funds. While the Company is still investigating the affected data, it included:

- Name, address, phone, and email;
- Masked Social Security (last 4 digits only);
- Masked bank-account numbers and some bank account identifiers;
- Government-ID images (e.g., driver's license, passport);
- Account data (balance snapshots and transaction history); and
- Limited corporate data (including documents, training material, and communications available to support agents).

The Company is continuing to review and bolster its anti-fraud protections to mitigate the risk that the compromised information could be used in social-engineering attempts. To the extent any eligible retail customers previously sent funds to the threat actor as a direct result of this Incident, the Company intends to voluntarily reimburse them after it completes its review to confirm the facts. The Company is also in the process of opening a new support hub in the United States and taking other measures to harden its defenses to prevent this type of incident.

While Coinbase has not experienced material operational impacts from these events as of the date hereof, the full financial impact of the Incident on the Company is still in the process of being assessed. Based on the information available to the Company on the date hereof and based on facts that continue to evolve, the Company has preliminarily estimated expenses to be within the range of approximately $180 million to $400 million relating to remediation costs and voluntary customer reimbursements relating to this Incident, prior to further review of potential losses, indemnification claims, and potential recoveries, which could meaningfully increase or decrease this estimate. The Company plans to aggressively pursue all remedies. As the Company's investigation is ongoing, the full impact of these events are not yet known.

Do investors care about cyber disclosures?

Badger et al. (2026)

New disclosure requirement **has not changed** how markets respond to these disclosures

Investors reward **disclosure completeness over speed**

Firms with a history of prior breaches experience more negative market reactions, consistent with disclosures **heightening perceived cybersecurity risk**

In Conclusion…

- Cybersecurity threats are increasing
- Cybersecurity is no longer just an IT problem
- Numerous ways for CPAs to protect ourselves and our clients
- Training, awareness, internal controls and disclosure are key

Andrea.Kelton@mtsu.edu