CPE Check-in

*Scan the QR code **or** enter the code IN THE EVENT APP:*

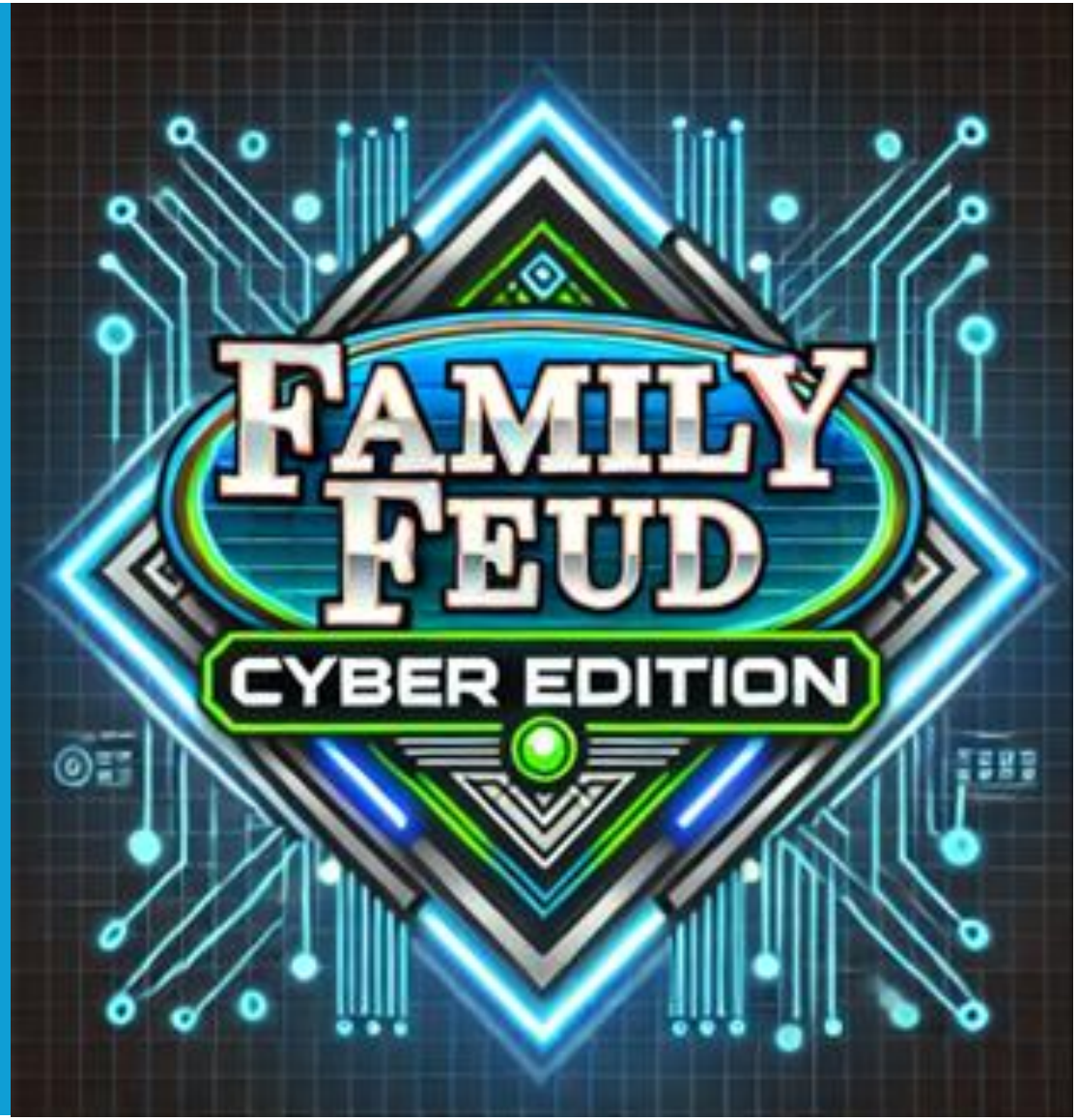
WHCEP5

North American Regional Conference 2025

Collaborate to Create: The Power of Strategic Alliances

Jason Gotway, Anders CPAs + Advisors
David Lam, Miller Kaplan
John Rostern, CBIZ

What happens if…. An interactive cybersecurity experience



The Power of Collaboration

Benefits to You

- Provide full spectrum of services
- Retain clients
- Grow service offerings
- Play bigger with more depth
- Improve infrastructure

CPA Firms without cybersecurity capability can leverage LEA to provide clients with assurance in this area.

Why Are We Here...

- LEA wants to foster collaboration with their members to enable growth, serve and retain clients and build relationships.
- We are here because we believe in this collaboration, and we have seen it work for all parties involved.
- If they aren't already, clients will be in need of cybersecurity services.
- And, if you don't have a way to serve this need, it may jeopardize the business that you do have with them.

Polling Question #1

Have any of your clients experienced a cyberattack or breach?

- Y or N

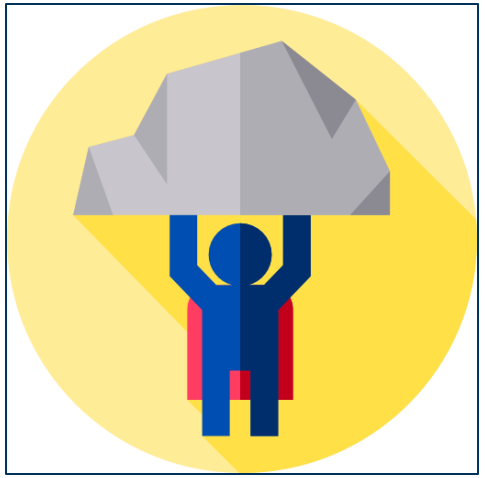
Polling Question #2

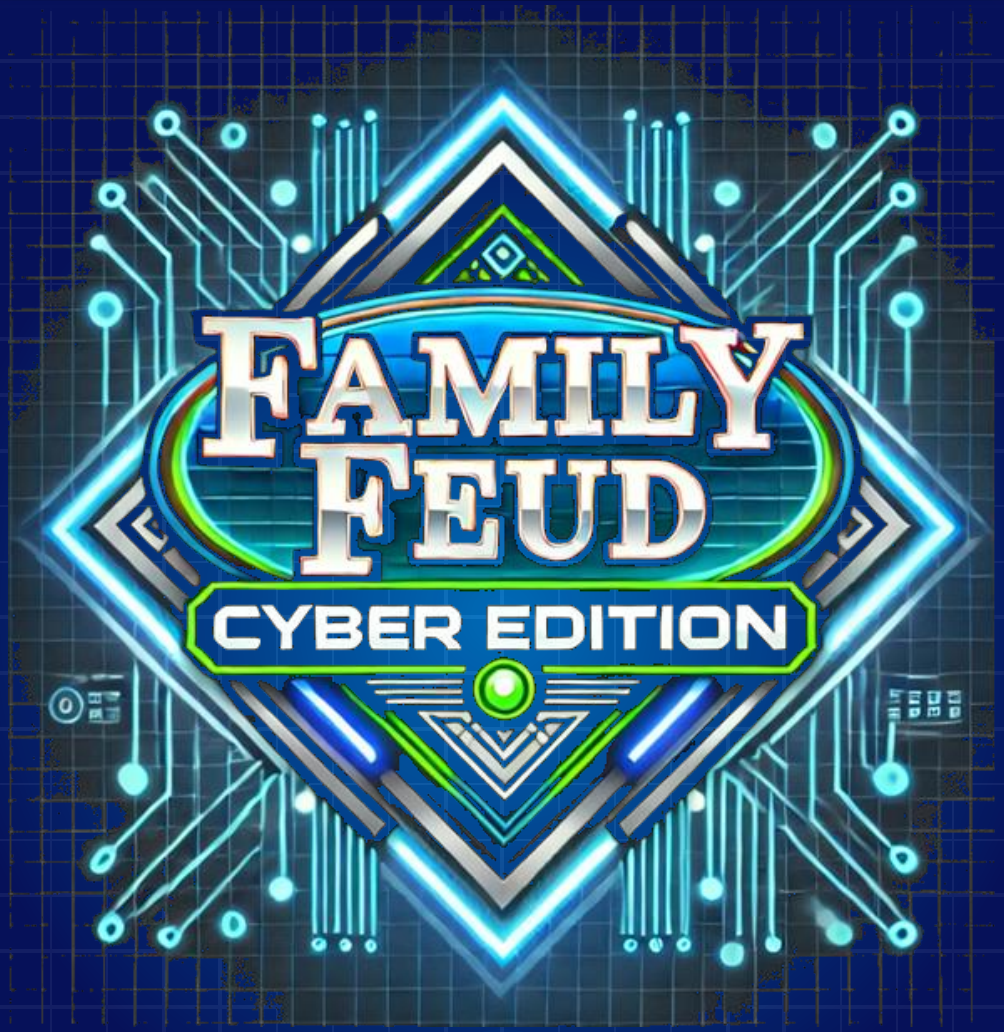
How many of your clients could go 19 days without their systems?

- Up to 25%
- 25-50%
- 50-75%
- 75-100%

Resiliency – Think About Your Clients

- How many days could our clients be down without data? Without systems?
- How much data could they lose and still operate their business?
- How many clients would they lose if their confidential data was exposed?




FAMILY
FEUD
CYBER EDITION

FAMILY FEUD
CYBER EDITION

Szczepaniak Escrow was founded in 1929 when Tony Szczepaniak had just graduated from college and earned his CPA. Tony believed in creating community, and continues to be a beloved leader, bringing people together all over the world. In 2024, Szczepaniak Escrow processed $5 billion in escrow funds through its accounts, setting an extraordinarily high bar for integrity and service

FAMILY FEUD
CYBER EDITION

On Friday at 2 PM, before heading to the airport to board a plane to Nashville, Tony had a call transferred from the front desk. It was the wealthy new owner of a house in St. Paul who used the escrow services. He told Tony that the previous owner of the house was refusing to hand over the keys because he never got the funds from Szczepaniak Escrow.

Tony unlocked his computer, because he is a believer in Information Security, and looked up the escrow. Why, he said, that's impossible. We transferred the $10 million in funds yesterday.

Immediately, Tony called together his team. Every single member of his staff was exceptional except for one team member.

Tony felt sorry for them, as they had unfortunately gone to Michigan State...

FAMILY FEUD
CYBER EDITION

What do you do?

Call the escrow officer to v[illegible]y the transaction occurred

Call [illegible] [illegible]ent

Call th[illegible] [illegible]eived

Pull up the receipt for the wire transfer

More information comes in…

- The wire transfer does indeed show that the bank received the money.
- Calling the receiving bank from the wire transfer shows that the bank is in Switzerland.
- The receiving bank will neither confirm nor deny that the funds were received.
- The escrow officer is unaware of anything unusual.

FAMILY FEUD
CYBER EDITION

What do you do?

Review the signed copies [illegible] identify the bank account

[illegible] the [illegible] [illegible] [illegible]

[illegible] [illegible] [illegible]

Review the email headers for signs of malicious activity

More information comes in…

- You find out that the signed documents differ in the original wire instructions from where the money was actually sent.
- Ashley, your team member from Michigan State, received an email with the wiring instructions change. She called the number on the email to verify via voice that it was actually the seller who made the instruction. She knew the seller personally, which is why she was comfortable verifying by voice.

FAMILY FEUD
CYBER EDITION

What do you do?

Execute your Incide Response (IR) plan

Revi logs rs mp ise’

3

earc in ation

Restrict communications on the incident to ‘need to know’

More information comes in…

- The user account for Josh Lampen, a recent college graduate who is a clerk and was CC'd on the transaction, was accessed starting three months ago from Russia.
- Josh's multifactor authentication, due to what is known in the company as Lampen complaining, was turned off because it was too hard to use.
- A rule existed in Josh's account automatically forwarding all email to a Gmail account.

What do you do?

Contact you ber insurer

Mo ll le il a nt

4

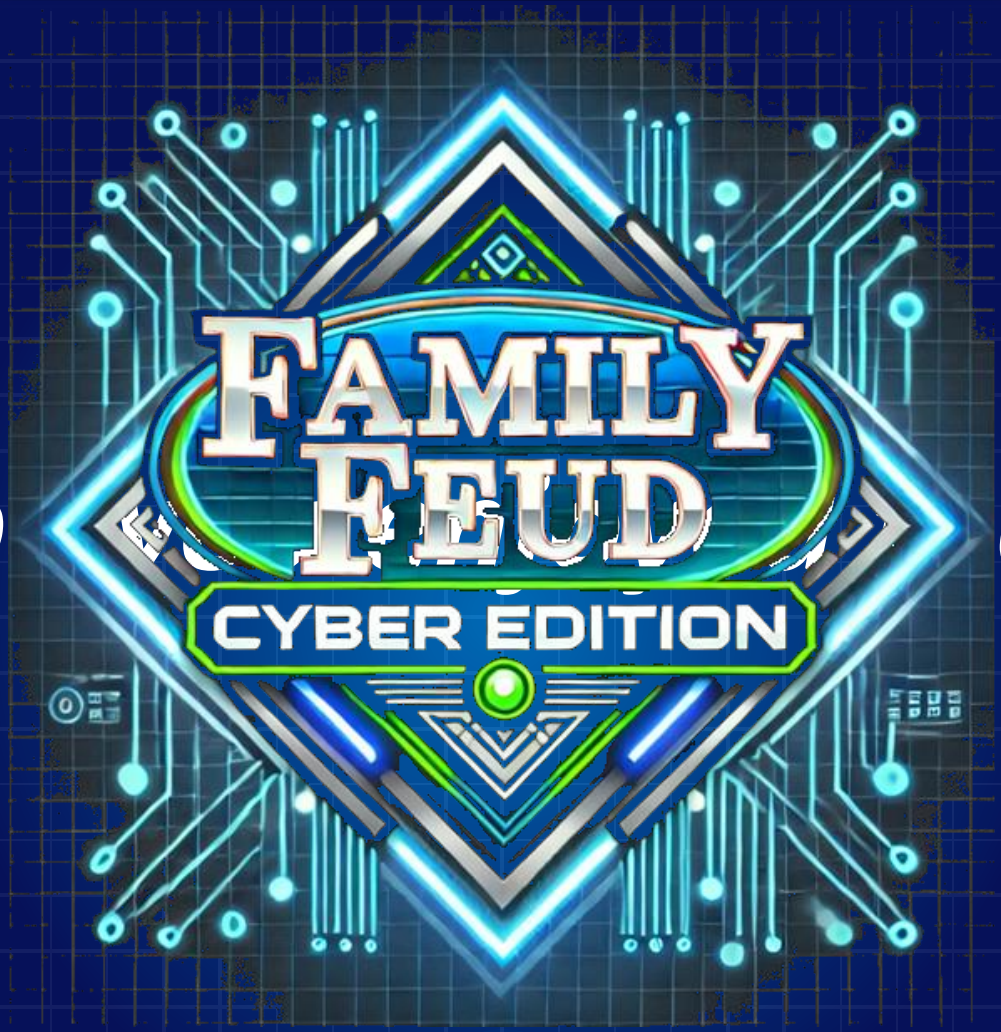
Make sure Multi Factor Authentication is enabled for all accounts

More information comes in…

- Your cyber attorney/breach coach instructs you to immediately contact your insurer and the FBI.
- Your bank tries, unsuccessfully, to claw back the money transfers.
- Forensic analysis indicates that a phishing attack led to credential compromise as the initial access method.

Lessons Learned

- Always enable Multi Fa[illegible]r Authentication (MFA)
- [illegible]Devel[illegible]ors
- [illegible]de [illegible]ishi[illegible]
- Implement ‘out of band’ verification procedures

We hop 

e show!

Questions

Thank You!

If today's conversation resonated with you and you'd like to explore it further, please reach out to one of us.

John Rostern

David Lam

Jason Gotway