Cybersecurity Risks of Fraudulent Payments

John Sutton, MBA, CPA, CPTM
CCFO Program Manager & Instructor
TCSA Fall Conference
November 22,2026

County Technical Assistance Service
INSTITUTE *for* PUBLIC SERVICE

Section 1 Cybersecurity Risks for Electronic Payments

FBI Statistics - 2024

68% of cyber fraud is **Business Email Compromise**

Cost $2.8 billion 2024

Losses: $10,000 to $4M

Ransomware inc. 74% from 2022 to 2023

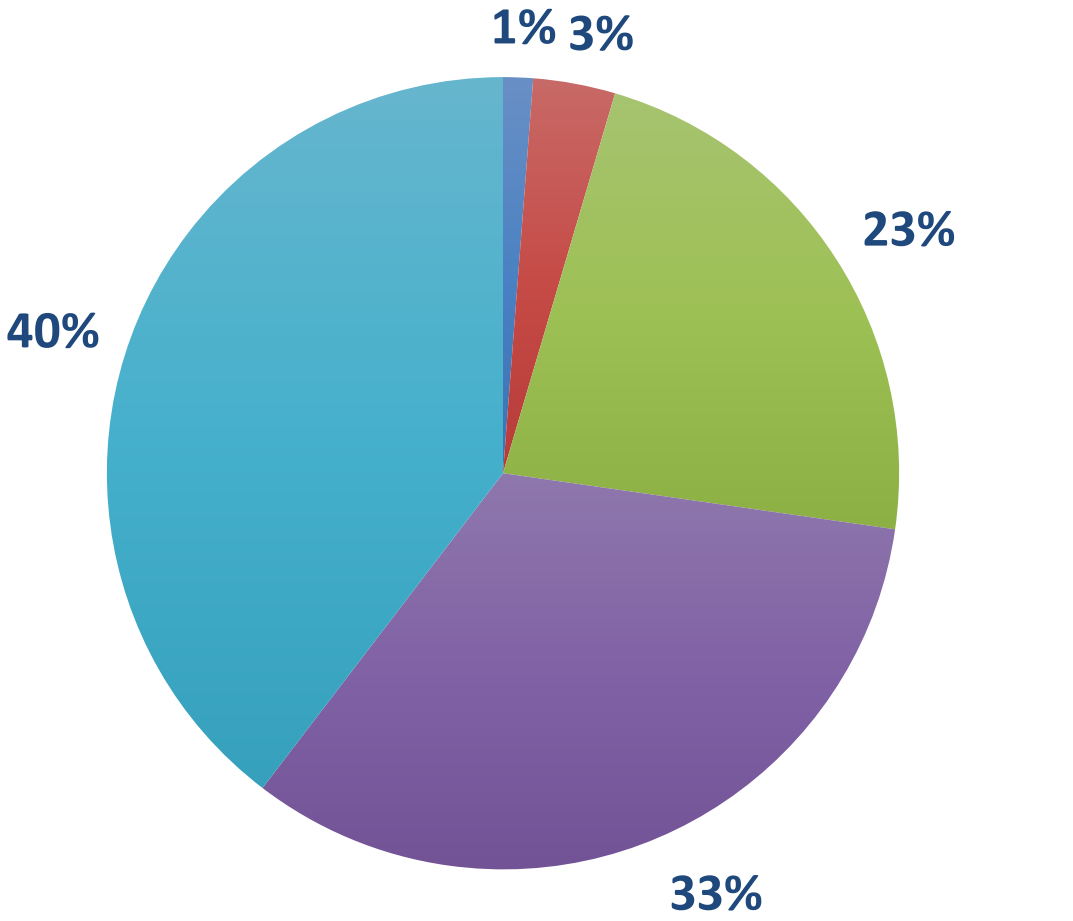
Change of payment method most common risk

Phishing

Vishing

TN is 19th of 50 U.S. State

FBI Statistics – 2024 (Cont.)



Total BEC Instances Nationally

Victim Age	# Instances	Damages
< 20 Years	90	$11.1 Million
21 to 29	800	30.6 Million
30 to 39	2,058	207.2 Million
40 to 49	2,934	302.4 Million
50 to 59	3,047	361.7 Million

Business Email Compromise (BEC)



Impersonating Vendor or Employee



Money Mule



Fraudsters as Mayor, Finance Director, or other official

BEC External Fraud

- BEC largest $ risk for external fraud
- FBI Public Service Video Message



Cybersecurity

Do you leave signed blank checks lying around?

Is your personal bank or credit card information protected & secure?

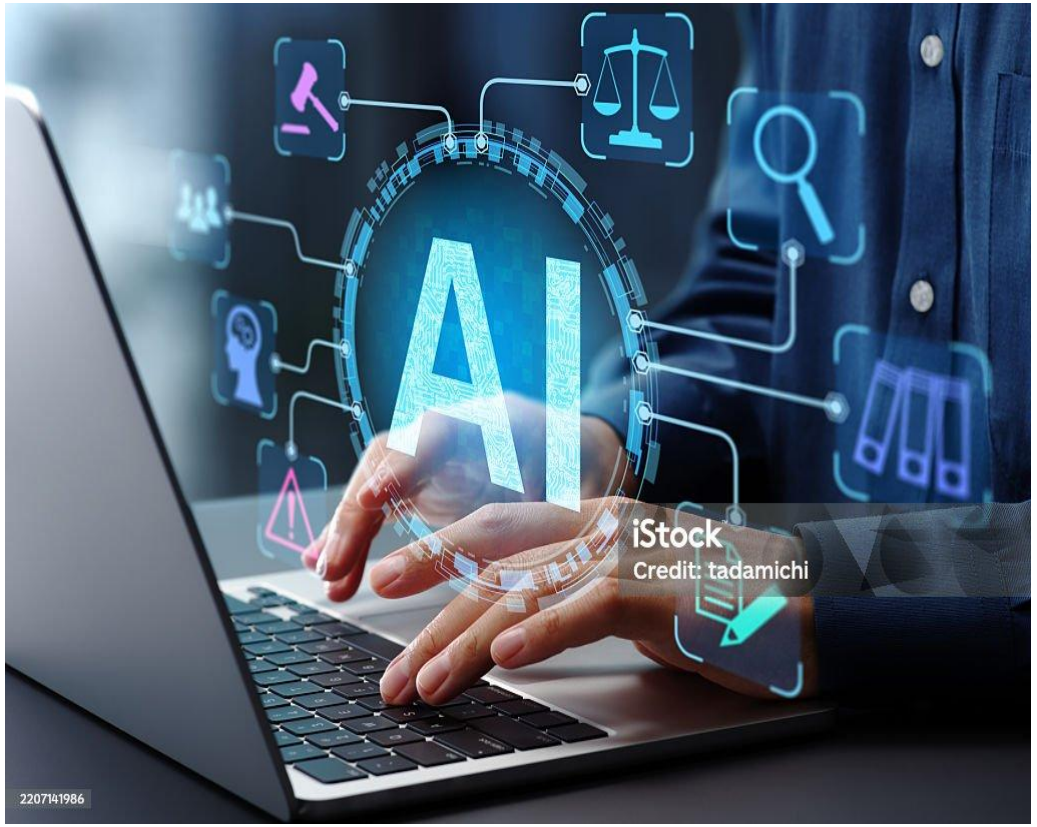
Are taxpayer funds secure?

Are you proactive or reactive?
Which one is cheaper?



Artificial Intelligence (AI) Risks

- Synthetic voices can imitate anyone
- Realistic social engineering
- Manipulating personal social information
- Accessing public information



Electronic Fund Transfer Act (EFTA) - Regulation E

Payment Initiated by County/City

EFTA Applies if account fraudulently charged externally

EFTA DOES NOT apply if County/City initiates payment

Counties are Targets



- Outdated technology
- Budget constraints
- Insufficient training
- Vendor information public
- Increasing electronic payments
- Failure to recognize risks

Fraudulent Payment Schemes

- **Phishing emails** impersonate vendor, employee, or official
- Target accounts payable, payroll, HR, or purchasing staff
- **Impersonate individuals** who have the authority to initiate & approve payments
- Email sense of urgency
- **AI increases risks** of impersonating vendors, banks, employees, and officials



Case Study #1 Tennessee County

Target: A 30-year experienced Finance Director/CPA and Mayor who was traveling out of the country.

Background: Criminals monitored Mayor's email & social media learned his email writing style and vacation plans. Obtained info on vendors from public records.

BEC Payment: Fraudsters sent phishing email (appeared legit) to finance director requesting $30,000 immediate payment to out-of-state vendor. Finance Director questioned the payment & called mayor's cell phone. After several email exchanges with the fictitious mayor over three days EFT payment was processed.

Result: County lost $30,000. No one checked original vendor files to call and verify request.

Case Study #2 North Carolina BOE

Target: N.C. BOE building new high school. Scammers sent phishing email to request change to bank account for EFT construction progress payments.

Background: The scammers email had the same logo and information as real vendor. The fraudsters signed and submitted the BOE forms to change their banking info.

BEC Payment: EFT payment of $2.5 million was sent. Legit contractor called several weeks later wanting to know when payment would be sent.

Result: Failed to call the contractor from original contract information to verify. BOE recovered $776K but lost $1.7 million.

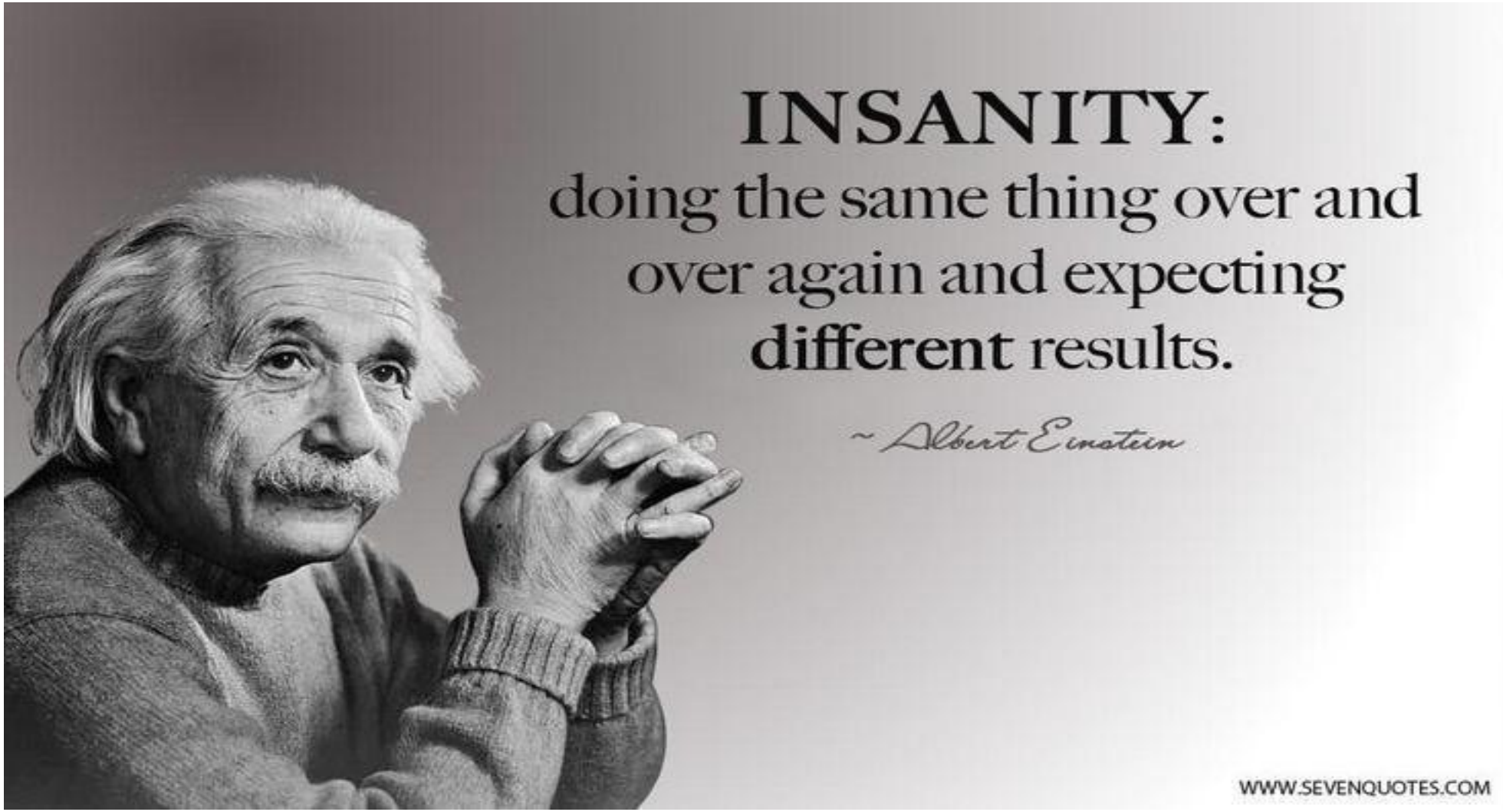
Case Study #3 Tennessee County BOE

Target: TN County BOE got phishing email from fraudster impersonating vendor requesting two EFT payments for $3.4M.

Background: Director of Schools & County Finance Director initially questioned this request. The fictitious email was the same as the actual vendor except the domain name was different by one letter.

BEC Payment: EFT payments of $3.4 million was sent to U.S. bank account of a "money mule". Bank notified the BOE of the fraud two weeks later.

Result: FBI investigation is continuing. To-date the BOE has recovered $742,000 from insurance and $2.4 million from U.S. banks. Remaining $300,000 is in process of recovery from U.S. bank. Failed to call & verify vendor from contract information.


INSANITY:
doing the same thing over and over again and expecting different results.
~ Albert Einstein
WWW.SEVENQUOTES.COM

Reduce Risks



Finance Director and County Trustee (2) approving wire transfers > $ limit AND approve change **payment methods/bank accounts. DOCUMENT!!!!**



Annual cybersecurity training for all employees: phishing emails, ransomware & other risks.



Update internal **control procedures to verify and confirm** requests for changes in payment methods and bank accounts.



Encrypted portal with **multifactor authentication (MFA)** for vendors & employees for sensitive information (banking, emails, contact info., etc.)

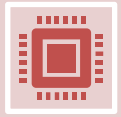
Reduce Risks (Cont.)



ACH and EFT bank filter **dollar limits**.



Require vendors & employees to **physically appear** with photo ID OR **verify with phone call** file information **NOT the email**!!!! **DOCUMENT**



Test defenses by **periodically testing your employees** with simulated cyber security attacks (phishing emails or ransomware).



New vendor require independent verification (website, phone call, and known references)

Local Government Corp (LGC) - Survey

Only 15% of LGC's customers use encrypted multi-factor authentication (MFA).

LGC offers additional protection for cybersecurity risks.

LGC
Local Government Corporation

FORTRESS
CYBERSECURITY SERVICES AND TOOLS
by LGC

SENTRY
Multi-Factor Authentication
Powered by Duo Security

Section 2 – Insurance and Conclusions

Cybersecurity Insurance

Unavailable or limited with high deductibles ($500,000+)

Rapidly increasing premiums

Lack of hardware and software **controls like VPN, dual authentication**, void/reduce insurance coverage

Higher coverage limits for catastrophic claim > $ limits

Coverage exclusions for damaged (corrupted) hardware and software

Volatile insurance market

Immediate Steps!!

Update internal controls - payee changes

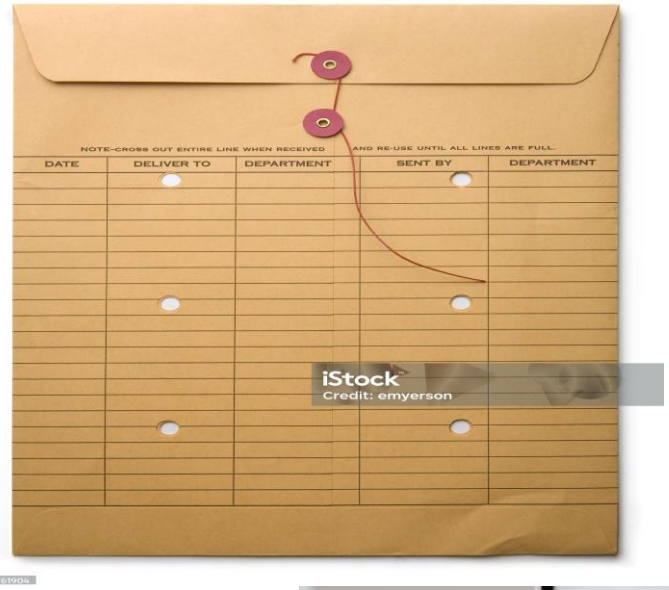
Training to change staff behavior

Physical Delivery - Inter-Office & U.S. mail

Verify ACH & EFT payments daily

In-person employee/vendor change (check photo IDs)

Phone call - original contract/HR info



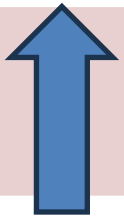


Conclusions

EFT and wire transfer payments will become more common

Proactive steps are cheaper than reactive

Scammers can read and copy your “open” emails

Vendor information is public information =  **RISK**

Conclusions (Cont.)



- Internal controls for 2 officials/managers required changing vendor & employee payments
- Use **encrypted VPN & multifactor (MFA) authentication** to secure emails
- **Change behavior** of officials and employees through constant training, education & cybersecurity testing
- **Positive pay** a must for checks

Free CTAS Cybersecurity Awareness Training:

1. Ten (10) **online** self-paced courses
2. Topics covered: **malware, phishing, social engineering**, internet safety, iPhone and mobile device safety
3. Earn 12.0 CPE Credits

https://www.ctas.tennessee.edu/training/catc

Contact Information:

John Sutton, CPA, CPTM, CCFO Program Manager and Instructor

Cell 865-963-5633

john.sutton@tennessee.edu

Contact your CTAS Consultant

References

1. Association of Finance Professionals (AFP) *2022 Payments Fraud and Control Report,* April 2022, JPMorgan Chase Bank
2. *Government Fraud Protection: A Strategic Imperative,* Wells Fargo Government Banking, 2024, Karekin Johnson
3. *North Carolina County lost $1.7 million in email scam,* STATESCOOP, August 2, 2019, Benjamin Freed
4. *What is Regulation E?,* Bankrate, August 29, 2024, Matthew Goldberg
5. *Cybersecurity Stats: Facts and Figures You Should Know,* Forbes Advisor, August 28, 2024, Mariah St. John

References (Cont.)

6. *Cyber Risk Savvy,* Government Finance Officers Association (GFOA), 2022, Shayne Kavanagh, Rob Roque, and Teri Takai

7. *Internet Crime Report,* U.S. Federal Bureau of Investigation (FBI), 2024, B. Chad Yarbrough