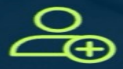
How AI, Deepfakes and ChatGPT are Transforming Cybercrime – and What to Do About It

THERESA PAYTON

Governance of AI

5 STEP FRAMEWORK



1

The Human User Story

Document customer centric and employee centric stories

2

Establish Safe AI Team

Leverage an existing council or set up a new one comprised of Line of Business Executives, Technology, Risk, Legal, Customer Service, Marketing, and Security - add other roles as needed

3

Create Pilot-Test-Learn

Ensure all AI implementations go through a pilot phase that tests out resiliency, reliability, privacy, security, and efficacy.

4

Trust but Verify

5

Deployment

CAN YOU DO

If You Can Only Do 1 Thing:

Design Around the Fraud – Do we allow internal passphrases to combat deepfake audio and video?

Three Questions About Generative AI

- Do we have a policy for employees and contractors regarding how to treat client and proprietary information?
- **Have we asked Generative AI about our company and our executives?**
- Do we have a policy if we find inaccuracies, personal information, client information within Generative AI?

Three Overall Questions You Can Ask

- Vendors and Supply Chain (Attestation)
- Is our cybersecurity roadmap comprehensive, resilient, and measurable – where does AI help or hurt?
- Do we have internal passphrases to combat deepfake audio and video?

My Favorite Free Tools

Review a link or attachment:
https://www.virustotal.com

Check for compromised accounts:

https://dehashed.com/

https://leakpeek.com/

https://haveibeenpwned.com/

Best Practices to Engage Government Resources

Foundational

- Discuss regulatory requirements with Internal Counsel. (Consider including Chief Risk or Chief Privacy Officer.)
- Reach agreement internally on LEO and Gov't Engagement Model.

Proactive Engagement

- Join FBI InfraGard.
- Request proactive briefings from your local FBI Field Office.
- Subscribe to FBI Bulletins and DHS CISA Bulletins. (Note: These agencies sometimes publish joint advisories.)

When in doubt, Call the FBI First

FBI Field Offices

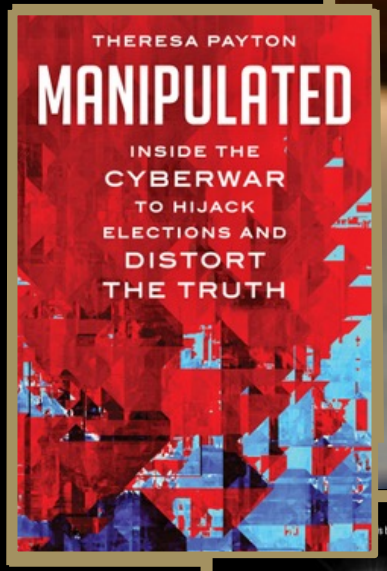
FBI at 1-800-CALL-FBI

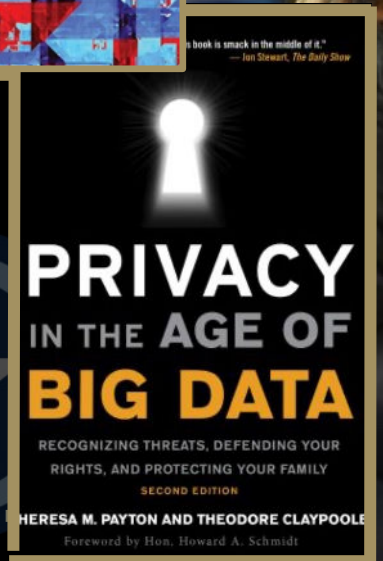
(1-800-225-5324)

Or https://bit.ly/3t2OlYl

The program's range of services include:

- ✓ Assistance with reporting cybercrime incidents to law enforcement agencies and other relevant organizations.
- ✓ Information and resources – training and education programs, technical assistance, and information sharing
- ✓ Referrals to support services, such as counseling or legal assistance.
- ✓ Support with recovering losses associated with cybercrime incidents.





Thank You!

Now, let's Keep the Conversation Going!

FortaliceSolutions.com

877.487.8160

Watchmen
@Fortalicesolutions.com

@TrackerPayton