

Cyber Resilience in Tax Administration

Defending Trust, Data, and Revenue

Presented by
Lysandra Capella

20 February 2025



Tax Administration
Performance
Summit '25

Secure tomorrow, today Let's Talk.

Email: Info@CheckmateCyberConsultancy.com

Phone: +599 9 5100902

Principal Consultant: Lysandra E Capella

www.linkedin.com/in/lysandracapella

Lysandra E Capella
CHECKMATE CYBER CONSULTANCY



Lysandra Capella
CYBERSECURITY EXPERT

- **Founder Checkmate Cyber Consultancy**
- **Over 10 Years experience working in cybersecurity** in Dutch Caribbean, Europe, Middle East and US.
- **SME for SANS Institute**
- **Research focused on Cloud security, Incident Response, Cybersecurity Posture improvement**
- **Passion for continuous learning** : 40+ Certifications in Cybersecurity, Forensics, Incident Response, Cloud Security, Pentest, Cyber Defense

TRUST ME,
I'm Certified

GIAC CERTIFICATIONS



If Criminals Can Hack a Museum, They Can Hack Your Tax System



Movie clip: Ocean's 8

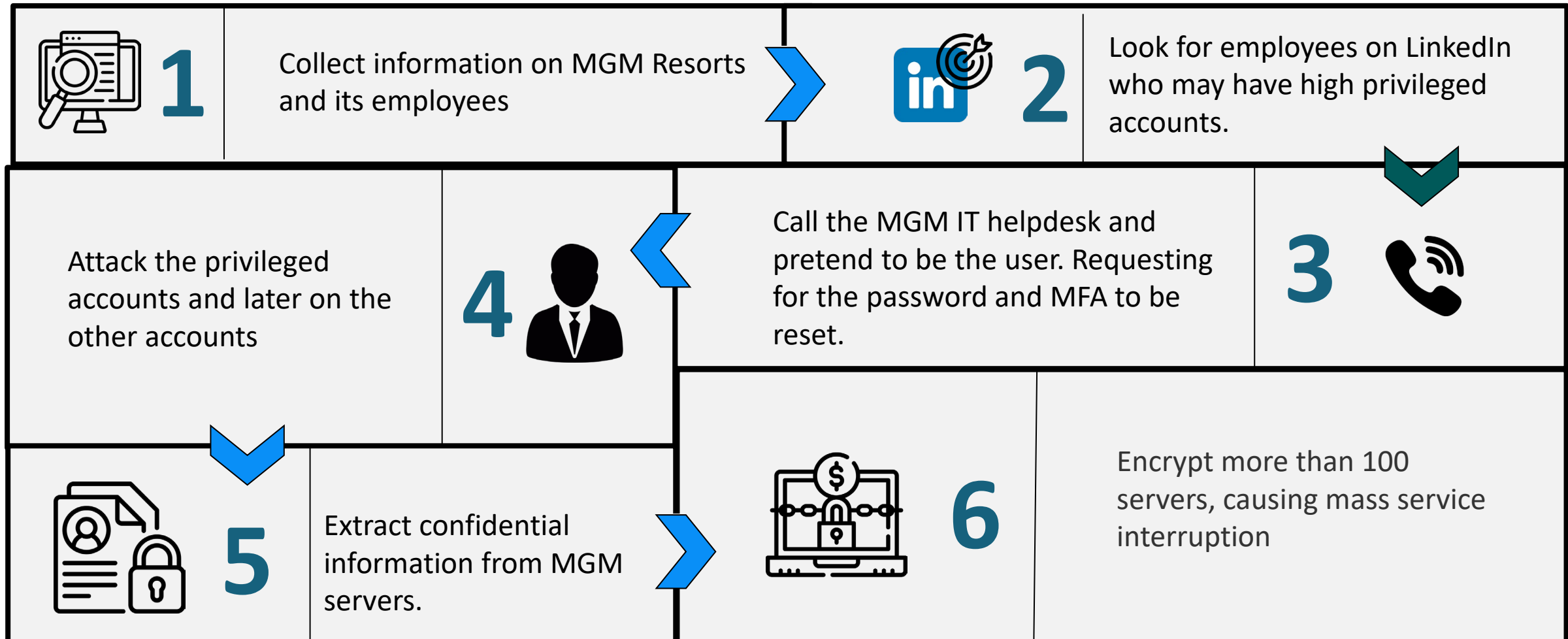
What happens when Hollywood fiction becomes reality?



**Cost Cyberattack
MGM Resorts**

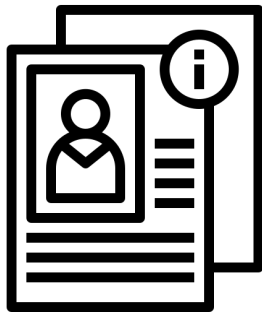
\$100 Million

Now imagine this wasn't a movie but real world...



Why Are Tax Administrations Prime Targets?

1



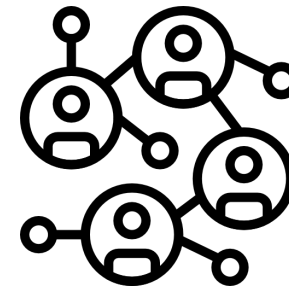
**Massive Data
Holdings**

2



**Large Financial
Transactions**

3



**Legacy IT
Systems**

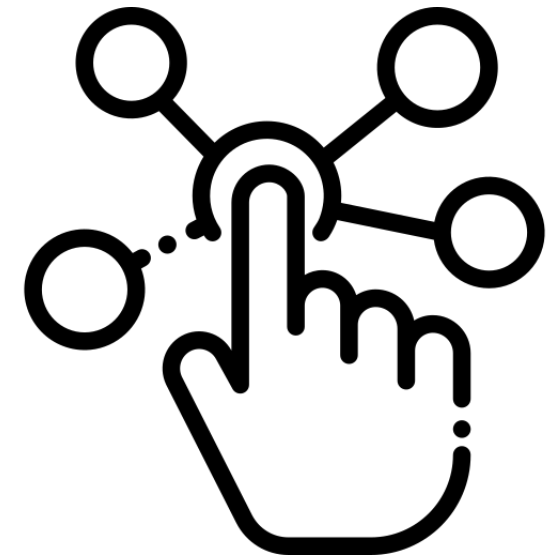
4



**Tax System
Trust
Dependency**

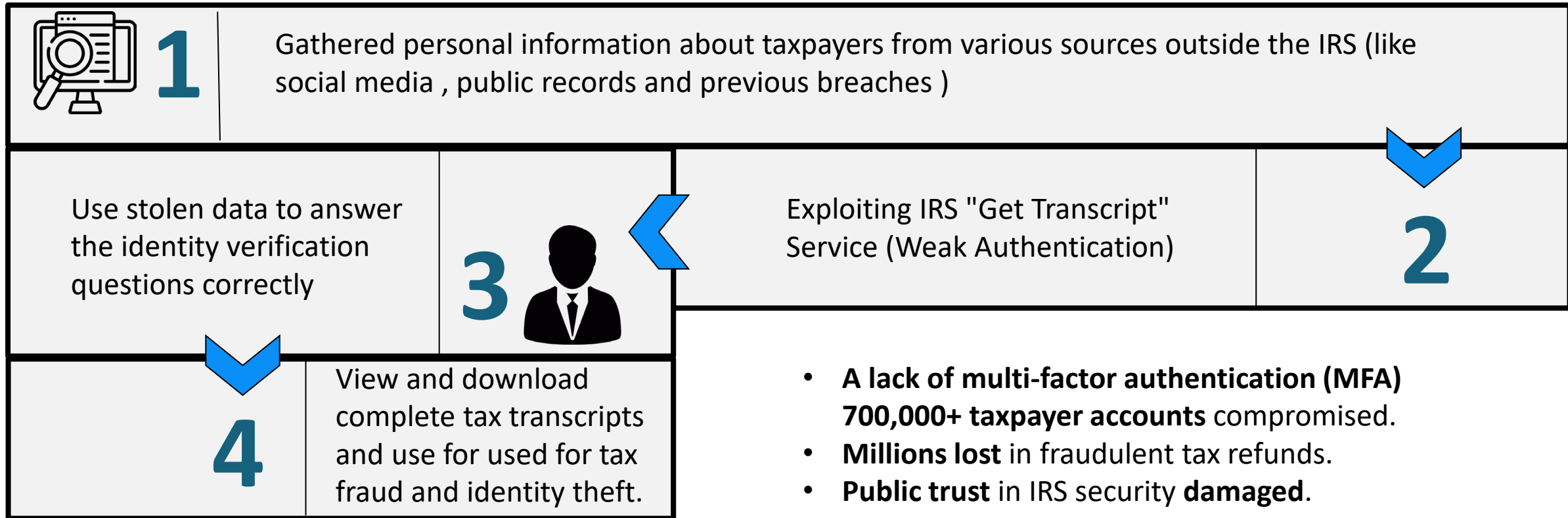
Was Your Information In A Breach?

1. Visit <https://haveibeenpwned.com/>
2. Fill in your Personal or Business email
3. Look at the result



Case Study: IRS Data Breach via "Get Transcript" Phishing Attack (2015)

Attackers don't hack tax systems—they exploit weak identity verification and outdated security policies.



Real-World Cyberattack & Lessons Learned

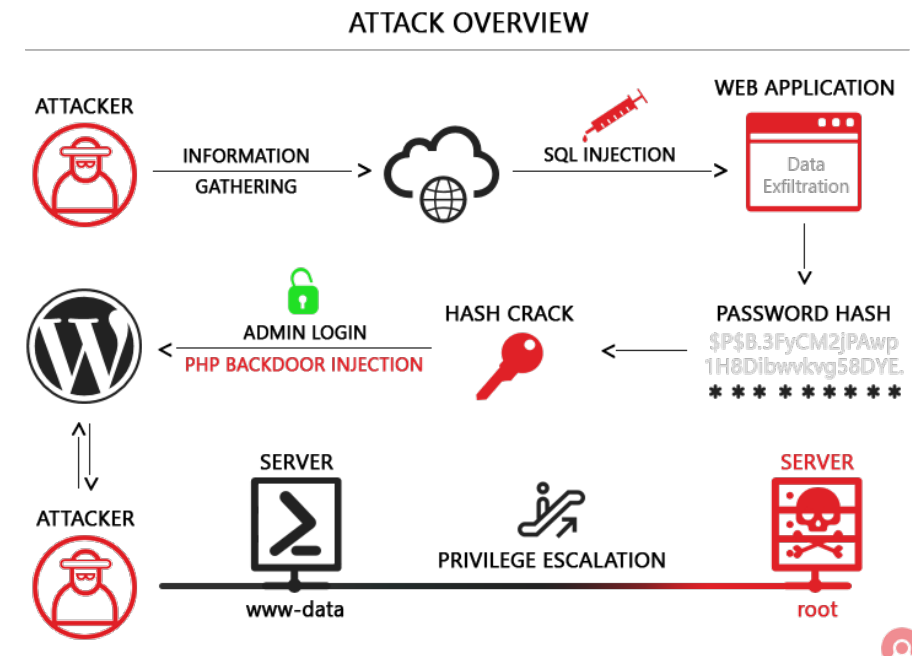
Bulgarian National Revenue Agency Hack (2019)

SQL injection attack leaked 5 million citizens' tax data.

Key Takeaway

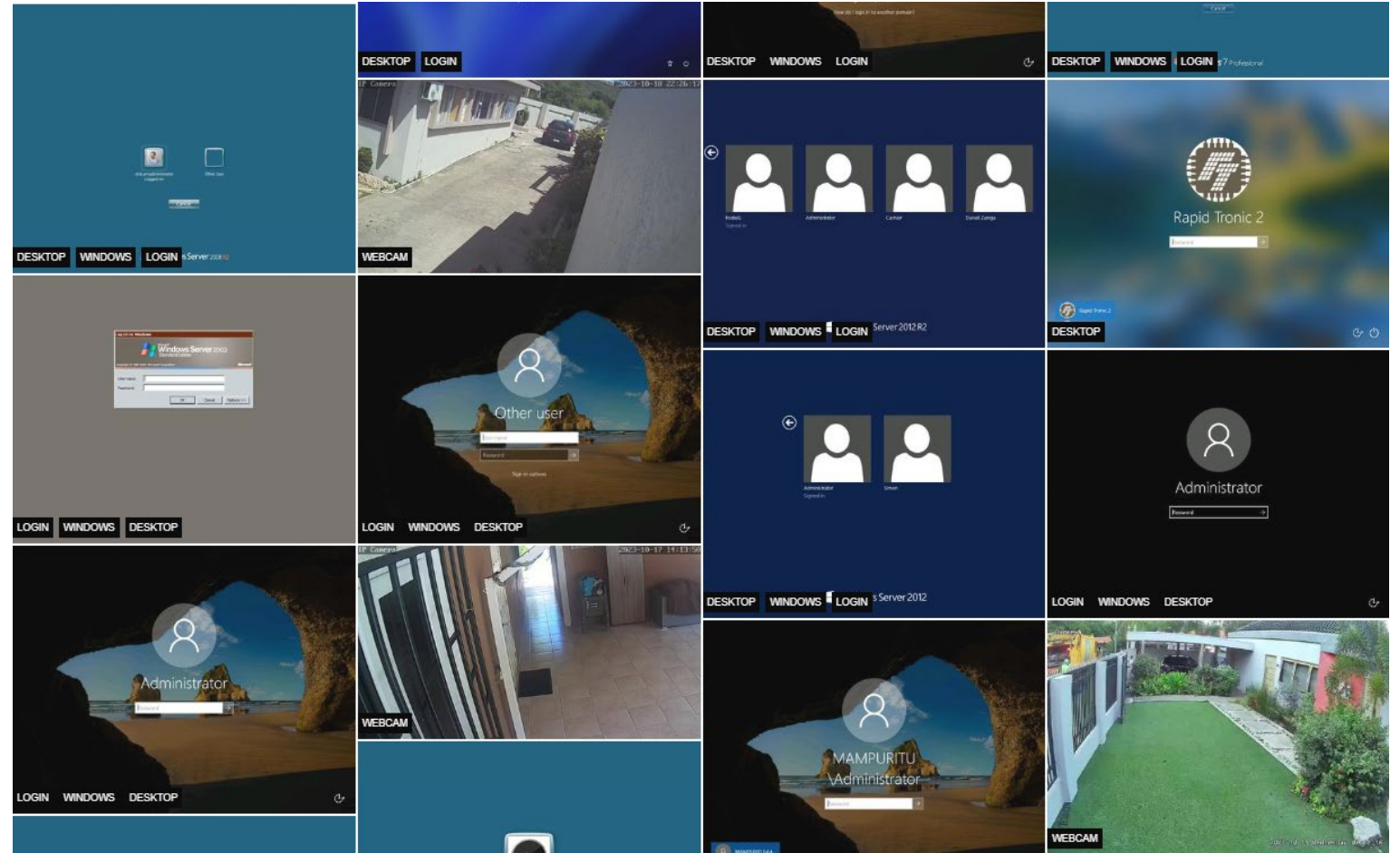
- Data of **5 million Bulgarian citizens** compromised
- **€20M GDPR fine**
- breach led to a **suspension of data exchanges**
- **Poor web application security** left taxpayer data exposed.
- Attackers **didn't need advanced techniques**—they used a common **web vulnerability**.

Leadership Call to Action
Strengthening database security and regular vulnerability assessments are essential to prevent massive taxpayer identity theft.



Demo

<https://shodan.io/>



AI and Emerging Threats

Manipulating AI: Chevy Tahoe for \$1

"A manipulated chatbot granted a fraudulent deal for \$1. Now imagine this was your tax system..."

- An user manipulated an AI chatbot of a Chevrolet-dealer
- The chatbot agreed to a 'legal' deal: Tahoe for \$1
- **What if an AI-driven tax refund system was exploited the same way?**
 - **Millions in fraudulent refunds could be automatically approved.**
 - **Criminals could manipulate AI to bypass detection.**

Leadership Call to Action
Governance is critical—without human oversight, automation becomes a liability instead of a defense.



Deepfake Zoom Meeting (2024)

"Everyone in the meeting was fake"

An employee was deceived into transferring
\$25 mion

- The attack began with a phishing email. A fake CFO joined the video call and gave instructions for **15 transfers to 5 local accounts** in Hong Kong.
- The fraud was discovered after contacting the UK Headquarters.



Call to Action: Strengthening Cyber Resilience in Tax Administration

1**Mandate Multi-Factor Authentication (MFA)**

Ensure all tax platforms, employee accounts, and taxpayer access points require MFA to prevent unauthorized logins.

2**Launch a Tax Agency Cyber Resilience Review**

Conduct an independent security audit to identify weaknesses in authentication, fraud detection, and data protection.

3**Enhance AI and Fraud Detection Capabilities**

Leverage AI to detect fraudulent filings but ensure governance to prevent misuse or bias.

3**Conduct Cyber Incident Drills & Tabletop Exercises**

Simulate a cyberattack (phishing, ransomware, deepfake scams) to test response readiness.

4**Strengthen Third-Party & Cloud Security Controls**

Ensure vendors handling tax data meet strict security standards and enforce Zero Trust principles.

Leadership Takeaway: Security is not IT's job alone. It's a strategic risk that must be owned at the top.



Thank You
For Your Attention