Cybersecurity and Your Role as a Tax Professional

- William “Bill” Odom

- Co-founder of Orbital Data Consulting
  - Digital Forensic Consulting
  - Cybersecurity Consulting
  - Expert Testimony
  - Electronic Discovery Services

- 25+ years DF / IR experience

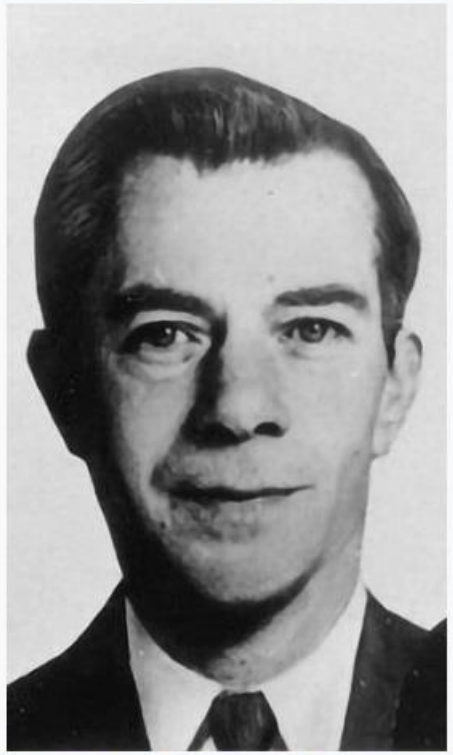
- Former FBI Special Agent and Big-4

- Testifying Expert in multiple jurisdictions

- Based in Houston, TX
  - *(Go Astros)*

- **Please ask questions!!!!**

Willie Sutton



FBI Ten Most Wanted Fugitive	
Charges	Bank robbery
Description	
Born	William Francis Sutton Jr. June 30, 1901 Brooklyn, New York
Died	November 2, 1980 (aged 79) Spring Hill, Florida
Status	
Added	March 20, 1950
Caught	February 1952
Number	11

Willie Sutton was a prolific bank robber and was the 11th person placed on the FBI's Ten Most Wanted Fugitive list

When asked by reporter Mitch Ohnstad why he robbed banks. According to Ohnstad, Willie Sutton replied, "***Because that's where the money is***".

Sutton later said that he never made this quote. That, while true, this quote was created by Ohnstad because it sounded better that Sutton's real quote and would sell more newspapers.

Sutton did admit to answering Ohnstad's question, though. "Why did I rob banks? Because I enjoyed it. I loved it. I was more alive when I was inside a bank, robbing it, than at any other time in my life. I enjoyed everything about it so much that one or two weeks later I'd be out looking for the next job. But to me the money was the chips, that's all."

The truth is, Threat Actors (commonly called "Hackers") apply both beliefs to their *"cause".* They infiltrate corporate and personal computer systems and networks because **they love the thrill and challenge** and because **that IS where the money is**!

ORBITAL


I DON'T ALWAYS THINK ABOUT
CYBERSECURITY
BUT WHEN I DO, IT'S USUALLY TOO LATE...

How many people here have been victims of cybercrime?

There isn't precise data on how many people are hacked in the US each year. However, here are some pubicly available statistics on cybercrime in the US:

- Data breaches: In 2022, there were 1,802 ***reported*** data compromises in the US, affecting over 422 million people.
- Cybercrime: In 2022, 53.35 million US citizens were affected by cybercrime.
- Cyberattacks: There are around 2,200 cyberattacks per day.
- Phishing attacks: In a six-month period, there were 255 million phishing attacks.
- Data breaches and exposure: In 2022, over 422 million people were affected by data breaches, leakage, and exposure.
- Cybercrime losses: Individuals lose $4,476 USD on average to cybercrime. **Business loss is more!**
- Phishing scams: Individuals of phishing scams lost $225 on average. **Business loss is more!**

ORBITAL

So, who is responsible for cybersecurity awareness?

IT?

End User?

C-Suite?

Service Providers & 3rd Parties?

CPA, Tax & Audit Firms?

Cybersecurity is <u>everyone's</u> responsibility because the digital world is interconnected, and the actions of one individual or organization can have far-reaching consequences

ORBITAL

1. **Data Protection**: Understand the importance of data protection and encryption to safeguard financial and personal data. Familiarize yourself with encryption protocols and data access controls.
2. **Phishing Awareness**: Teach your team and clients how to recognize phishing emails and other social engineering tactics used by cybercriminals.
3. **Multi-Factor Authentication (MFA)**: Promote the use of MFA for all accounts, especially for financial systems and email. MFA adds an extra layer of security by requiring multiple forms of identification to access an account.
4. **Password Management**: Encourage strong password policies, password managers, and regular password changes. Weak passwords are a common entry point for hackers.
5. **Incident Response**: Develop a well-defined incident response plan for dealing with data breaches or cyberattacks. This should include steps to contain, mitigate, and recover from an incident.

6. **Data Backup and Recovery:** Ensure regular data backups and test the restoration process. A solid backup strategy can help recover from data loss due to cyberattacks or hardware failures.

7. Cybersecurity Training: Train your staff on basic cybersecurity practices, including email security, internet use, and secure file sharing.

8. Secure File Sharing: Implement secure methods for sharing sensitive files with clients and colleagues, such as encrypted cloud storage or secure file transfer systems.

9. Cloud Security: Understand the security features and risks associated with cloud-based accounting software and storage solutions. Assess the security of third-party cloud providers.

Cybersecurity is a critical concern for public accountants as you handle sensitive financial and personal information. Staying up to date with the latest cybersecurity topics is essential to protect client data and maintain the trust of your clients. Here are some important cybersecurity topics for public accountants to consider:

10. Regulatory Compliance: Keep up to date with industry-specific regulations (e.g., GDPR, HIPAA) and ensure compliance when handling client data.

11. Third-Party Risk Management: Evaluate the cybersecurity practices of third-party vendors or service providers who have access to your client's data. Ensure they meet your security standards.

12. Remote Work Security: With an increasing trend toward remote work, accountants should be knowledgeable about securing remote access to company resources.

13. Cyber Insurance: Consider investing in cyber insurance to help mitigate financial losses in case of a data breach or cyberattack.

14. Penetration Testing and Vulnerability Scanning: Regularly assess your network and systems for vulnerabilities by conducting penetration tests and vulnerability scans.

15. Employee Monitoring and Insider Threats: Be aware of the risks of insider threats and the importance of monitoring employee activity to detect potential security issues.

16. Legal and Ethical Aspects: Familiarize yourself with the legal and ethical implications of cybersecurity, including client confidentiality and disclosure requirements.

17. Cybersecurity Frameworks: Consider implementing cybersecurity frameworks like NIST Cybersecurity Framework or ISO 27001 to establish a structured approach to cybersecurity.

Cybersecurity is a critical concern for public accountants as you handle sensitive financial and personal information. Staying up to date with the latest cybersecurity topics is essential to protect client data and maintain the trust of your clients. Here are some important cybersecurity topics for public accountants to consider:

Staying updated on these cybersecurity topics and continuously educating yourself and your team is crucial for public accountants to protect client data and maintain the integrity of financial information.

Cybersecurity is a critical concern for public accountants as you handle sensitive financial and personal information. Staying up to date with the latest cybersecurity topics is essential to protect client data and maintain the trust of your clients. Here are some important cybersecurity topics for public accountants to consider:

ORBITAL

1. **Tax-Related Scams**: During tax season, accounting firms are often targeted with tax-related scams, such as fraudulent tax returns or tax evasion claims, which can damage the firm's reputation and client trust.
2. **Phishing Attacks:** Phishing remains a significant threat. Attackers often send convincing emails posing as clients, colleagues, or financial institutions to trick accountants into revealing sensitive information or clicking on malicious links.
3. **Ransomware:** Ransomware attacks have become ***more sophisticated***. Attackers use encryption to lock accountants' files and demand a ransom for decryption keys. Firms are advised to have strong backup and recovery strategies to mitigate the impact.
4. **Business Email Compromise (BEC):** BEC attacks involve compromising email accounts to conduct fraudulent transactions, ***including wire transfers***. Attackers may impersonate company executives or clients to request funds transfers
5. **Insider Threats:** Malicious or negligent employees can pose a significant threat to accounting firms. Insider threats can involve data theft, fraud, or accidental data exposure.

What are the current trends in cybersecurity threats and attacks targeting accounting firms?

ORBITAL

What are the current trends in cybersecurity threats and attacks targeting accounting firms?

This is NOT a complete list of Current Trends. Other trends include:

- Supply Chain Attacks
- Credential Theft
- Social Engineering Attacks
- Cloud Security Concerns
- Legal and Regulatory Risks

Given the evolving nature of cybersecurity threats, it's essential for accounting firms to regularly update security measures, conduct risk assessments, and invest in cybersecurity awareness and training for employees.

Additionally, staying informed about the latest threats and following best practices is crucial in maintaining a strong security posture.

It's recommended to consult with cybersecurity experts and consider engaging in threat intelligence sharing networks to stay ahead of emerging threats.

AICPA & the IRS have useful and FREE cybersecurity awareness resources.

What is your role as a tax professional regarding cybersecurity?

1. **Training and Awareness:**
   - Conduct training sessions for clients' employees to raise awareness about cybersecurity best practices.
   - Educate clients on how to recognize and respond to common cyber threats like phishing and social engineering.

2. **Incident Response Planning:**
   - Assist clients in developing an incident response plan to minimize the impact of a data breach or cyberattack.
   - Ensure that clients have a clear process for reporting and addressing security incidents.

3. **Regular Audits and Monitoring:**
   - Perform periodic cybersecurity audits to identify and rectify vulnerabilities.
   - Set up continuous monitoring systems to detect and respond to security incidents promptly.

4. **Assessment and Risk Analysis:**
   - Conduct cybersecurity assessments to identify potential vulnerabilities and risks within the client's financial systems.
   - Perform risk analysis to determine the impact of a security breach on the client's business and its financial data.

5. **Security Policies and Procedures:**
   - Assist clients in developing and implementing comprehensive cybersecurity policies and procedures tailored to their specific needs and risks.
   - Provide guidance on password policies, data encryption, access controls, and other security measures.

CPA firms can (and arguably should) play a crucial role in helping clients practice safe cybersecurity, especially since you deal with sensitive financial and personal information.

Here are several ways in which CPA firms can assist clients in this regard:

6. **Secure Data Handling:**
   - Advise on secure data storage, transmission, and disposal methods, ensuring client data is protected at all stages.
   - Recommend encryption and secure file-sharing solutions for sensitive financial information.
7. **Compliance Assistance:**
   - Help clients understand and comply with relevant regulations, such as the General Data Protection Regulation (GDPR) or the Health Insurance Portability and Accountability Act (HIPAA), depending on their industry.
8. **Vendor Risk Management:**
   - Help clients assess and manage the cybersecurity risks associated with third-party vendors and service providers they use for financial or operational purposes.
9. **Documentation and Compliance Records:**
   - Help clients maintain proper documentation of cybersecurity measures and compliance efforts for auditing purposes.
10. **Encourage a Security Culture:**
    - Promote a culture of cybersecurity within the client's organization, emphasizing the importance of security awareness and vigilance.

CPA firms can (and arguably should) play a crucial role in helping clients practice safe cybersecurity, especially since you deal with sensitive financial and personal information.

Here are several ways in which CPA firms can assist clients in this regard:

Who is responsible for cybersecurity awareness?

Cybersecurity is <u>everyone's</u> responsibility because the digital world is interconnected, and the actions of one individual or organization can have far-reaching consequences

By providing these services and guidance, CPA firms can contribute to the clients' overall cybersecurity posture, safeguarding sensitive financial data and helping to prevent financial and reputational damage resulting from cyber incidents.

It's essential to stay proactive and adapt to evolving cybersecurity threats and regulations to provide the best protection possible.

ORBITAL

Questions?

William Odom

Co-Founder at Orbital Data Consulting,
Member CEO Vistage Group (Houston)

- ***Bill Odom – Contact Info***
- Email: wfo@orbital.global
- Mobile: +1 713 927 5377
- Office: +1 346 352 8876
- Website: www.orbital.global
- LinkedIn:
  - https://www.linkedin.com/in/williamodom/