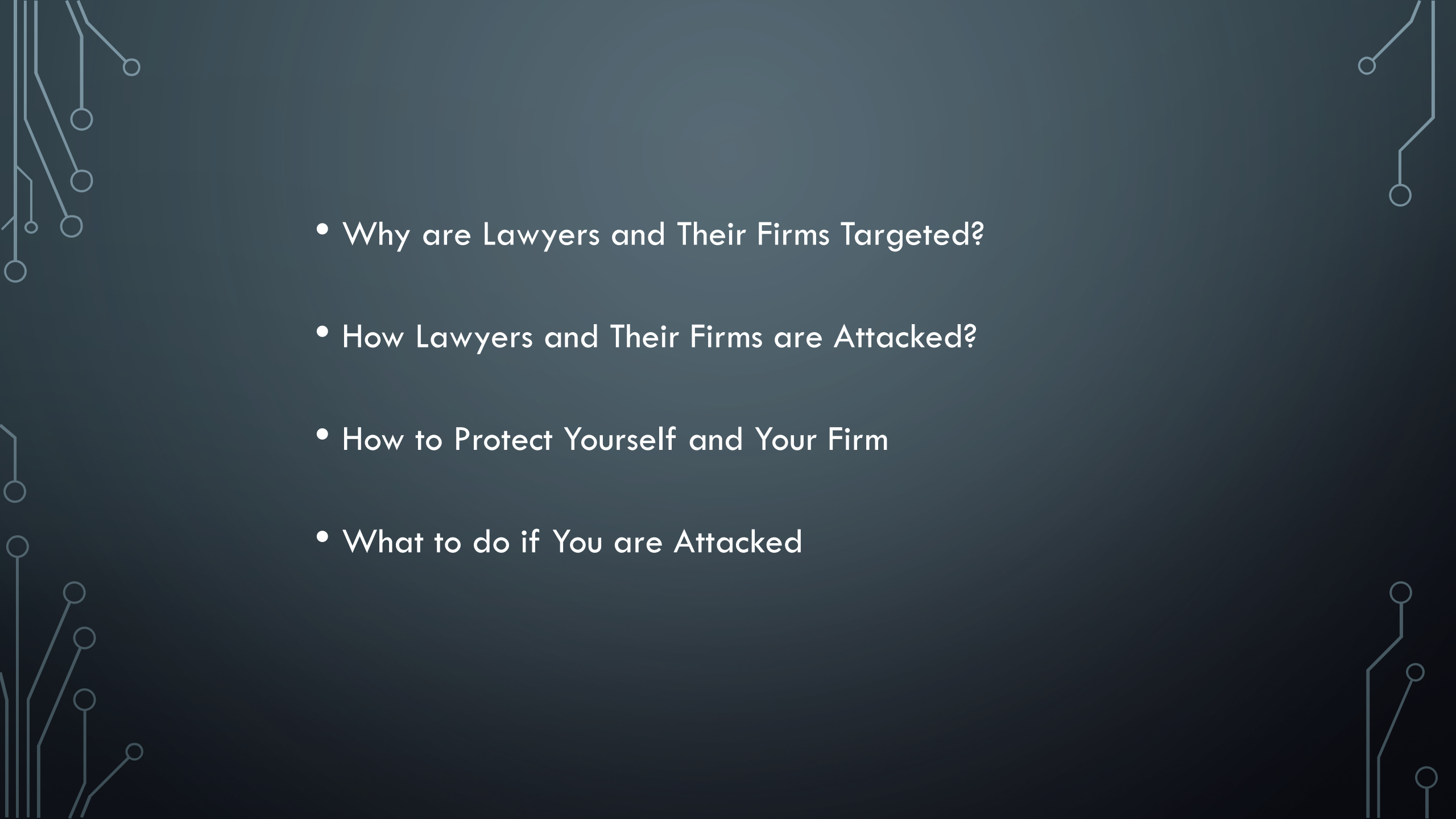




Anatomy of a Law Firm Cyber Breach

William Weicker
System Security Specialist

- 
- Why are Lawyers and Their Firms Targeted?
 - How Lawyers and Their Firms are Attacked?
 - How to Protect Yourself and Your Firm
 - What to do if You are Attacked

WHY ARE LAWYERS AND LAW FIRMS TARGETED?

- General Malicious Intent
- Clients Personal Information
- Financial Gain

HOW ARE LAWYERS AND THEIR FIRMS ATTACKED?

- Online Research
- Phishing Schemes
- Ransomware
- Unsecured Networks

Phishing Schemes

Phishing is one of the easiest and most common form of a cyber attack. Its usually done over email but can also be found on social media sites. This type of attack is meant to gather information or trick the user into installing Malicious Software

Ransomware

Ransomware is a form of Malware that prevents users from accessing data or systems.

Ransomware can encrypt Backup Files, Shadow Copies, and even External or Network Drives. However, not all Ransomware encrypts data.

<https://www.nomoreransom.org/en/index.html>

<https://www.avast.com/en-us/ransomware-decryption-tools>

Unsecured Networks

An Unsecure Network most often refers to public WiFi or Hot Spots. Connecting to an Unsecure Network can give nearby Hackers the ability to eavesdrop on your connection giving them the ability to intercept your login credentials, Data, and even installing Malicious Software.

HOW TO PROTECT YOURSELF AND YOUR FIRM

- Secure Backups
- Compliance Testing
- SSAE 18 (SOC Types 1 & 2)
- Penetration Testing

Compliance Testing

- Phishing Testing
- Websites & Links
- Unknown Downloads
- Unsecured/Unauthorized Devices

What to do if You or Your Firm is Attacked

- Notify IT personnel
- Quarantine Effected Systems From Network
- Investigate the Source of the Breach/Attacker