American Bar Association - Resolution 609

# Major Cyber Threats

## 1 RANSOMWARE

A form of malware (malicious software) that attempts to encrypt (scramble) your data and then extort a ransom to receive a decryption key that will unlock your data.

## 2 PHISHING

Emails appearing to be from legitimate sources to trick employees into clicking on malicious links or downloading malware. Links or attachments can give cybercriminals access to the law firm's computer systems.

## 3 SOCIAL ENGINEERING

Impersonating a client or employee, to gain the trust of employees and trick them into revealing sensitive information or providing access to computer systems.

## 4 DATA LEAKAGE

Theft and misplacement of small mobile devices.

## 5 UNSECURED NETWORKS

Cybercriminals can gain access to law firms' computer systems through unsecured wireless networks, especially those that do not require a password or use weak encryption.

## 6 WEAK PASSWORDS

Cybercriminals can use brute-force attacks or passwordguessing techniques to gain access to law firms' computer systems, especially if employees use weak or easily guessable passwords.

## 7 MALWARE

Cybercriminals use various types of malware, such as viruses, trojans, and ransomware, to gain unauthorized access to law firms' computer systems. Once installed, malware can steal data, destroy files, or provide backdoor access to cybercriminals.

## 8 THIRD-PARTY VENDORS

Cybercriminals can access law firms' computer systems through third-party vendors or contractors that have access to the firms' systems. If these vendors or contractors have weak security measures in place, cybercriminals can use their access to infiltrate the law firms' systems.

## 9 INSIDER THREATS

If your organization employs staff (full time or as contractors), they might leak data by mistake or maliciously.