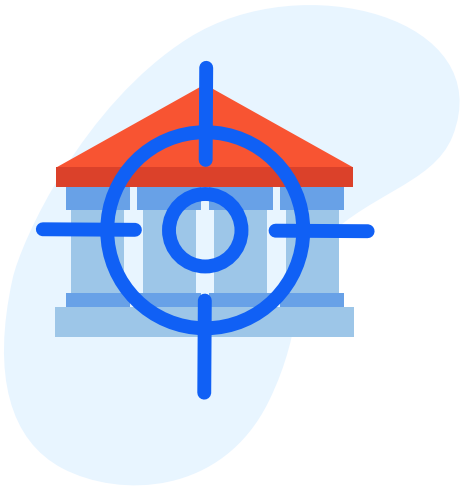
6 CRITICAL CYBERSECURITY & COMPLIANCE FACTS FOR LEGAL ORGANIZATIONS

In the competitive legal industry, client confidence in their data's safety can differentiate you. Here are six cybersecurity and compliance facts every law firm must know.



1 More Frequent Targets for Cyberattacks

The rate of cyberattack incidents is growing year-over-year, with up to 42% of law firms with up to 100 employees having experienced a data breach, according to the American Bar Association (ABA).

2 All Sizes Are a Target

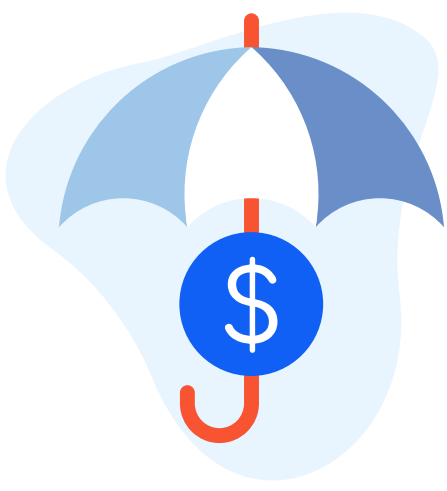
Due to the extremely sensitive nature of information processed at law firms, even smaller local practices must handle the consequences of cyberattacks. Smaller organizations are preferred targets for hackers because of:

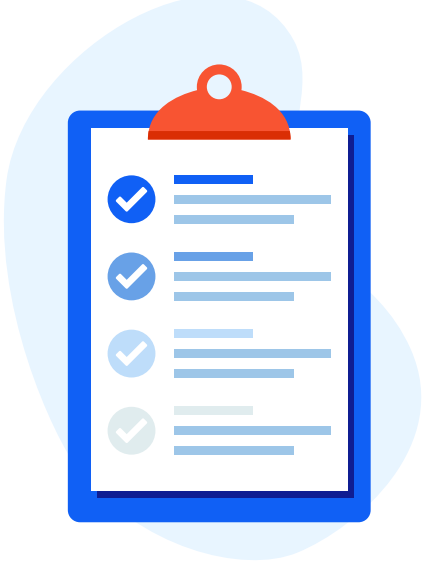
- **Valuable Data**
- **Perceived Weaker Security**
- **Limited Cybersecurity Resources & Expertise**
- **Use of Standard Commercial Software**
- **Lack of Awareness & Training**
- **Compliance Pressures**
- **The Ripple Effect**
- **Increased Use of Technology**

Example: The law firm Moses Afonso Ryan Ltd., based out of Providence, Rhode Island, had critical financial files locked down by cybercriminals for three months after a ransomware attack in 2016. The firm's billing system and billing-related documents were locked down, so clients could not pay the firm and financial information was inaccessible. The law firm was forced to negotiate a ransom in Bitcoin at an undisclosed cost. Over $700,000 was lost in client billings for the firm due to the attack, plus any possible new business that could have been closed during those three months.

3 The Cost of a Breach Far Exceeds the Cost of Prevention

According to IBM's 2023 Cost of a Data Breach Report, the average data breach cost for professional services organizations, which encompasses law firms, is $4.47 million. In comparison, small to medium-sized businesses typically only spend 10% of their annual IT budget on cybersecurity.





4 Compliance Obligations Are Growing

Law practices have additional requirements to protect information classified under specific categories. The list of compliance regulations is extensive and includes, but is not limited to:

- **American Bar Association (ABA) Model Rules of Professional Conduct Formal Opinions 477R and 483**
- **Health Insurance Portability and Accountability Act (HIPAA)**
- **Payment Card Industry Data Security Standard (PCI DSS)**
- **Sarbanes-Oxley Act (SOX)**
- **General Data Protection Regulation (GDPR)**
- **National Institute of Standards and Technology (NIST)**
- **FTC Safeguards Rule**

5 Cyber Insurance is Not Enough

While important, cyber insurance does not prevent data breaches, and insurance providers are well aware of this. High-quality safeguards on your network are critical to obtaining or keeping cyber insurance. Insurance providers can deny coverage to companies not meeting minimum standards to prepare for and defend against cyberthreats. Specific criteria may vary slightly by provider, but typically, four types of security controls are required to qualify:

- **Multi-Factor Authentication (MFA)**
- **Security Awareness Training**
- **Encrypted Backups**
- **Endpoint Detection & Response (EDR)**

6 Cybersecurity Measures Don't Need to be Disruptive

Modern cybersecurity solutions are designed to integrate seamlessly with daily operations. Applicable examples to your business include:

Email Encryption

Implementing email encryption is a simple process that works in the background to secure communications without altering the user experience.

Two-Factor Authentication (2FA)

While adding an extra step to the login process, 2FA significantly enhances security with minimal impact on user access times.

Automated Backups

Automated, regularly scheduled data backups ensure data integrity without disrupting work, protecting against data loss scenarios.

Enhance your legal organization's security affordably with TPx's specialized cybersecurity expertise. TPx helps hundreds of legal customers with compliance and cybersecurity, freeing up your team's time for strategic tasks. TPx offers HIPAA, PCI DSS and SOC 2-compliant solutions and has a security advisory team specializing in helping legal organizations with various compliance needs through a service like VCO (virtual compliance officer).

See How TPx Helps Legal Organizations Stay Secure and Compliant

LEARN MORE

TPX

www.tpx.com