FUSION Computing
416-566-2845
www.FusionComputing.ca

LEGAL

Law firms are often victims of cyberattacks because they have sensitive (and valuable) information about multiple companies or entities, usually housed in a single database. This makes firms "one-stop shops" for cybercriminals since they can obtain the desired data on various companies via a single source.

Some Key Areas To Review:

PHISHING

Cybercriminals contact users, impersonating legitimate business contacts.

Lures targets into giving up sensitive data and access to company resources.

REMOTE TEAMS & VIRTUAL MEETINGS

Video conferencing software has become increasingly mainstream.

Adopt security controls, including requiring participants to register and authentication to maintain privacy.

If accessing sensitive client data outside the office, implement secure connections and a VPN.

Cyber security insurance provides an additional level of security for firms that suffer from a data breach. While insurance does little to protect the stolen data, some policies do compensate for certain financial impacts of a breach, such as any fees associated with restoring the data, loss of income due to downtime, crisis management, or forensic Investigations.

CENTRALIZED CLIENT DATA

It's the digital equivalent of putting all of your eggs in one basket.

Sensitive data is housed in a single encrypted location, making it easier for criminals to target.

DEVICE SECURITY

Unauthorized access to computers or devices may lead to compromise of sensitive and important information.

Physical techniques can be used to hack a device.

Users may leave a device unattended while traveling or working in another area, leaving the device susceptible to a hacker.

Implement device security baseline policies such as auto timeout, password policies, MFA, SSO, and more.

FUSION Computing

LEGAL

Key NIST/CyberSecure Canada control points:

SECURE MESSAGING

Email is a primary means of communication within legal organizations.

Mailbox storage capacities tend to grow with the constant addition of sensitive data.

The implementation of email security policies, email storage limits, and email best practices.

SECURITY AWARENESS

Educate staff and end users about cybersecurity.

Staff require regular security awareness trainings.

Test staff progress and knowledge by deploying phishing campaigns.

MANAGED ENDPOINT DETECTION & RESPONSE

A technically strong team of analysts reviewing EDR data, determining which pieces are useful and which aren't.

The security Operations (SOC) team will respond to identified threats automatically.

Works with an antivirus solution to provide extra protection by finding evidence of compromise and detecting malicious behaviour.

PASSWORDS & AUTHENTICATION

Require employees to change passwords regularly, require strong passwords and use them properly

Enforce Multi-factor authentication, requiring more than one authentication mode before accessing data

PATCH MANAGEMENT

Ensure all software and hardware are regularly patched and updated.

Updates often are issued to address security issues and a failure to apply patches can leave your firm vulnerable.

FUSION COMPUTING targeted remediation:

RISK ASSESSMENTS

Risk must be gauged based on factors such as probability of occurrence, impact on the organization, and prioritization.

Risk assessments should be conducted or reviewed regularly and at least once per year.

SECURITY CONTROLS

- Anti-virus and MDR
- Secure encrypted backups
- Data Loss Prevention
- Encryption at rest and in transit
- Firewall
- Incident Response Plan
- Mobile Device Management
- Policies and procedures
- Security Awareness Training
- Vulnerability Management
- Multi-Factor Authentication

CIS Controls