absolute it
Information Technologies

Legal IT Security Checklist

Professional Cybersecurity & Technology Risk Assessment Guide for Sydney Law Firms

Prepared by Absolute IT Consulting

Table of Contents

Introduction

Technology has become central to the operation of modern law firms.

From client communications and confidential documents to billing systems and remote access, nearly every part of a legal practice depends on secure and reliable IT systems.

Unfortunately, many firms only discover weaknesses in their cybersecurity or IT infrastructure after a serious issue occurs.

Cybersecurity incidents, downtime, phishing attacks, data breaches, and unreliable support can disrupt operations, damage client trust, and expose firms to financial and reputational risk.

This booklet was created to help Sydney law firms evaluate the security, reliability, and operational readiness of their current IT environment.

Whether you currently work with an internal IT team or outsourced provider, this checklist will help you identify common gaps that may be putting your firm at unnecessary risk.

Why Cybersecurity Matters for Law Firms

Law firms are increasingly targeted by cybercriminals because they store:

- Confidential client information
- Financial records
- Legal documentation
- Sensitive communications
- Commercial agreements
- Identity data

Attackers understand that legal practices often cannot afford downtime or data exposure.

Even a small disruption can affect:

- Client confidence
- Billable productivity
- Court deadlines
- Regulatory obligations
- Business continuity
- Reputation

Strong cybersecurity is no longer optional.

It is now a core operational requirement for protecting your clients, staff, and business.

Is Your Law Firm Actually Protected?

Most law firms assume their technology is secure until something goes wrong.

The reality is that many legal practices operate with hidden cybersecurity risks, outdated systems, weak access controls, and unreliable backup processes, leaving client data exposed.

Because law firms handle highly sensitive information, they are increasingly targeted by phishing attacks, ransomware, business email compromise, and credential theft.

This checklist will help you identify common technology and cybersecurity gaps that could put your firm at risk.

Use this guide to evaluate your current IT environment and determine whether your systems, staff, and security processes are adequately protecting your firm.

Legal IT Security Checklist

1. Multi-Factor Authentication (MFA)

Do you have MFA enabled for:

- ☐ Microsoft 365 accounts
- ☐ Remote access/VPN access
- ☐ Email accounts
- ☐ Cloud applications
- ☐ Practice management software
- ☐ Administrator accounts

Warning Signs

- Staff can log in with only a password
- MFA is optional instead of enforced
- Shared user accounts exist
- Partners bypass security requirements

Why It Matters

Password theft is one of the most common causes of breaches in the legal industry. MFA dramatically reduces the risk of unauthorised access to client data and email systems.

---

2. Email Security & Phishing Protection

Is your firm protected with:

- ☐ Advanced spam filtering
- ☐ Anti-phishing protection
- ☐ Email impersonation protection
- ☐ Attachment scanning
- ☐ URL protection
- ☐ Staff phishing awareness training

Warning Signs

- Staff regularly receive suspicious emails
- No phishing simulation training exists
- Employees click unknown links frequently
- Email accounts have been compromised previously

Why It Matters

Law firms are heavily targeted because attackers know legal staff handle confidential documents, financial information, and sensitive communications.

---

3. Backup & Disaster Recovery

Do you have:

- ☐ Automated daily backups
- ☐ Offsite/cloud backups
- ☐ Immutable or ransomware-protected backups
- ☐ Backup monitoring
- ☐ Tested recovery procedures
- ☐ Documented disaster recovery plans

Warning Signs

- Backups are “assumed” to work but never tested
- One person is solely responsible for backups
- Recovery times are unknown
- Critical systems cannot be restored quickly

Why It Matters

A backup is only valuable if it can be restored quickly during a crisis.

Many firms discover backup failures only after ransomware or server outages occur.

---

4. Endpoint Protection

Are all firm devices protected with:

- ☐ Modern antivirus/EDR protection
- ☐ Centralised monitoring
- ☐ Automatic security updates
- ☐ Device encryption
- ☐ Remote device management
- ☐ Threat detection tools

Warning Signs

- Staff use unmanaged personal devices
- Devices fall behind on updates
- No visibility into laptop security status
- Lost devices cannot be remotely wiped

Why It Matters

Every laptop, desktop, and mobile device connected to your systems can become an entry point for attackers.

---

5. User Access Controls

Does your firm:

- ☐ Remove access immediately when staff leave
- ☐ Restrict access based on job role
- ☐ Avoid shared accounts
- ☐ Require strong password policies
- ☐ Audit privileged/admin access regularly
- ☐ Review user permissions routinely

Warning Signs

- Former employees still have active accounts
- Staff have unnecessary admin privileges
- Multiple people share credentials
- Access reviews never occur

Why It Matters

Too much access creates unnecessary risk and increases exposure if accounts are compromised.

---

6. Microsoft 365 Security

Is Microsoft 365 configured securely with:

- ☐ Conditional access policies
- ☐ MFA enforcement
- ☐ Audit logging enabled
- ☐ Secure mailbox settings
- ☐ External sharing controls
- ☐ Data loss prevention policies

Warning Signs

- Microsoft 365 was set up with default settings
- External file sharing is unrestricted
- No monitoring of suspicious sign-ins exists
- Legacy authentication is still enabled

Why It Matters

Many breaches occur because Microsoft 365 environments are poorly configured, not because the platform itself is insecure.

---

7. Cybersecurity Policies & Staff Training

Does your firm provide:

- ☐ Cybersecurity awareness training
- ☐ Acceptable use policies
- ☐ Remote work security guidelines
- ☐ Password management standards
- ☐ Incident response procedures
- ☐ Ongoing employee education

Warning Signs

- Staff have never received cyber training
- Security policies are outdated or missing
- Remote workers use insecure home setups
- Employees do not know how to report incidents

Why It Matters

Human error remains one of the leading causes of cybersecurity incidents.

---

8. Secure Remote Work

Are remote staff protected with:

- ☐ Secure VPN access
- ☐ Managed devices
- ☐ MFA enforcement
- ☐ Encrypted laptops
- ☐ Secure file-sharing tools
- ☐ Remote monitoring and support

Warning Signs

- Staff use personal devices for firm work
- Sensitive files are stored locally
- Home networks are unmanaged
- Remote workers bypass security controls

Why It Matters

Hybrid work environments create additional exposure if remote access is not properly secured.

---

9. Vendor & Third-Party Risk

Has your firm evaluated:

- ☐ Cloud vendors
- ☐ Software providers
- ☐ IT support vendors
- ☐ Data-sharing partners
- ☐ Third-party security practices
- ☐ Vendor access permissions

Warning Signs

- Vendors have unrestricted access
- No vendor security review process exists
- Contracts lack cybersecurity requirements
- Third parties access sensitive client data unnecessarily

Why It Matters

Your firm's security is only as strong as the vendors connected to your systems.

---

10. Incident Response Readiness

Does your firm know:

- ☐ Who to contact during a cyber incident
- ☐ How systems would be restored
- ☐ How staff should respond to suspicious activity
- ☐ What legal/compliance obligations apply
- ☐ How clients would be notified if necessary
- ☐ How quickly operations could recover

Warning Signs

- No documented response plan exists
- Leadership has never rehearsed a cyber scenario
- Recovery responsibilities are unclear
- Staff panic during technical incidents

Why It Matters

A fast, organised response can dramatically reduce downtime, financial loss, and reputational damage.

Quick Self-Assessment

Score Your Firm

Give yourself:

- 1 point for every section fully addressed
- 0 points if gaps exist

8 – 10 Points

Strong security foundation with good operational maturity.

5 – 7 Points

Moderate risk exposure. Improvements recommended.

0 – 4 Points

High risk exposure. Significant gaps may leave your firm vulnerable.

Common Signs Your Law Firm Has Outgrown Its Current IT Provider

- Slow response times during urgent matters
- Recurring issues
- Poor communication from support
- No proactive cybersecurity guidance
- Lack of strategic planning
- Frequent staff complaints about systems
- Growing uncertainty around compliance and security
- Reactive support instead of prevention

If these sound familiar, your current IT support may no longer meet the needs of a growing legal practice.

How Absolute IT Consulting Helps Sydney Law Firms

At Absolute IT Consulting, we help law firms:

- Reduce cybersecurity risk
- Improve reliability and uptime
- Protect sensitive client data
- Support hybrid and remote work securely
- Eliminate recurring technology frustrations
- Improve response times and accountability
- Keep teams productive and supported

We understand the urgency, confidentiality, and operational demands legal firms face every day.

Ready to Identify Your Firm's Risks?

Schedule a discovery call with us to review your current environment, identify security gaps, and discuss how to improve reliability, responsiveness, and protection across your firm.

Website: https://www.absoluteitconsulting.com