Cybersecurity Assessment - 5 Critical Questions

5 Critical Security Areas Every Law Firm Should Evaluate

How to Use this Assessment

Rate each area below as STRONG (fully documented and current), NEEDS WORK (partially addressed), or MISSING (outdated or not documented). Your answers will reveal your firm's cybersecurity readiness and priority areas for improvement.

IMPORTANT DISCLAIMER: This assessment provides cybersecurity guidance only, and does not constitute legal, compliance, or insurance advice. Consult qualified legal counsel and insurance professionals for specific regulatory requirements and coverage details in your jurisdiction.

1 RISK ASSESSMENT DOCUMENTATION

Can you provide a current, documented cybersecurity risk assessment specific to your firm?

What This Means:

- Annual formal assessment of your firm's specific cyber risks
- Documented inventory of systems, data types, and vulnerabilities
- Written analysis of threats relevant to your practice areas
- Board or partner-approved risk tolerance statements

Industry Best Practice: Documented risk assessments demonstrate due diligence and informed decision-making about security investments. Many firms find this supports their efforts to meet "reasonable efforts" standards, though specific legal requirements vary by jurisdiction.

Red Flags:

- No formal assessment in the past 12 months
- Generic risk assessments not tailored to legal practice
- Risk assessment that doesn't address client data specifically
- Assessments done by IT vendor without legal industry expertise

Your Status: ☐ **STRONG** ☐ **NEEDS WORK** ☐ **MISSING**

2 EMPLOYEE SECURITY TRAINING DOCUMENTATION

Do you have documented, completed security training for all employees with measurable outcomes?

What This Means:
- Formal training program covering legal-specific cyber threats
- Completion certificates and attendance records
- Phishing simulation testing with documented results
- Training content updated annually to address current threats

Industry Best Practice: Many cyber insurance underwriters now request evidence of ongoing security awareness training. Legal industry best practices suggest demonstrating employee competency in protecting confidential information.

Red Flags:
- One-time training sessions without follow-up
- Generic corporate training not specific to legal threats
- No documentation of completion or effectiveness
- Training that doesn't include phishing simulation testing

Your Status: ☐ **STRONG** ☐ **NEEDS WORK** ☐ **MISSING**

3 EXTERNAL THREAT MONITORING

Do you actively monitor for compromised credentials, external vulnerabilities, and dark web exposure?

What This Means:
- Continuous monitoring of dark web for firm and employee credentials
- External vulnerability scanning of internet-facing systems
- Attack surface monitoring beyond your internal network
- Documented response procedures for discovered threats

Industry Best Practice: Proactive threat detection represents an evolution beyond reactive incident response. Many insurance providers recognize external monitoring as evidence of comprehensive security practices.

Red Flags:
- Relying only on internal security monitoring
- No dark web credential monitoring
- Unknown external attack surface exposure
- No documented process for responding to external threats

Your Status: ☐ **STRONG** ☐ **NEEDS WORK** ☐ **MISSING**

4 INCIDENT RESPONSE DOCUMENTATION

Do you have a documented, tested incident response plan specific to client data breaches?

What This Means:
- Written procedures for responding to cyber incidents
- Client notification templates and timelines
- Bar association reporting requirements documented
- Legal counsel contact information for breach response
- Regular testing and updates of response procedures

Industry Best Practice: Many states have specific breach notification procedures. Professional liability policies often reference documented incident response capabilities. Industry best practices suggest having prompt action procedures for protecting confidential information.

Red Flags:
- Generic incident response plans not specific to legal requirements
- No client notification procedures documented
- Untested response procedures
- No legal counsel identified for breach response

Your Status: ☐ **STRONG** ☐ **NEEDS WORK** ☐ **MISSING**

5 VENDOR RISK MANAGEMENT

Do you have documented security requirements and monitoring for all technology vendors with access to client data?

What This Means:
- Written security requirements for all technology vendors
- Regular security assessments of key vendors
- Contractual security obligations and liability provisions
- Documentation of vendor access to client information

Industry Best Practice: Legal industry standards suggest ensuring vendors implement appropriate protections for confidential information. Many cyber insurance policies reference vendor risk management practices.

Red Flags:
- No written security requirements for vendors
- Cloud services without security documentation
- Vendors with access to client data but no security agreements
- No regular review of vendor security practices

Your Status: ☐ **STRONG** ☐ **NEEDS WORK** ☐ **MISSING**

SCORING YOUR ASSESSMENT

Calulate your total score
- STRONG = 2 points
- NEEDS WORK = 1 point
- MISSING = 0 points

8-10 points: Excellent Cybersecurity Position

Your firm demonstrates comprehensive security documentation practices. Focus on maintaining current standards and staying updated with evolving threats.

Potential Next Steps:
- Schedule annual reviews of all documentation
- Consider advanced threat intelligence services
- Evaluate potential cyber insurance benefits

5-7 points: Moderate, Gaps Need Attention

Your firm has some solid security practices but important gaps remain. Priority should be on strengthening weak areas quickly.

Potential Next Steps:
- Address MISSING areas within 90 days
- Upgrade NEEDS WORK areas to STRONG status
- Consider cybersecurity consulting to accelerate improvements

0-4 points: Immediate action needed

Your firm may face significant security and liability exposure. Immediate action is recommended to address documentation gaps.

Potential Next Steps:
- Begin with formal risk assessment within 30 days
- Implement employee training program immediately
- Consult with cybersecurity specialists
- Review professional liability insurance coverage

CRITICAL REFLECTION

After completing this assessment, ask yourself: **If you are entrusted with client personal information, private data and/or intellectual property, are you taking all reasonable measures to protect it?**

Your assessment results provides a clear picture of where your firm stands. Now you must decide what you will do with that information. This is where Guardian can help.

- **Documentation and compliance tracking** for risk assessments and regulatory requirements
- **Behavioral security training programs** that focus on changing habits, not just awareness
- **External threat monitoring** that identifies risks before they reach your internal systems

Ready to strengthen your cybersecurity position?

INDUSTRY BENCHMARKS

Based on industry surveys and compliance reviews:
- Most law firms lack current risk assessments
- The majority cannot document completed security training
- Few have external threat monitoring
- Many lack tested incident response plans
- Most have inadequate vendor risk management

The firms that excel in all five areas often experience:
- Potential cyber insurance benefits
- Smoother client proposal processes
- Reduced regulatory audit concerns
- Better competitive positioning for enterprise clients

IMMEDIATE ACTION ITEMS

If you marked any area as MISSING:
1. Schedule a cybersecurity consultation to understand security best practices and timelines
2. Review your cyber insurance policy to understand current coverage and requirements
3. Identify your biggest vulnerability and address it within 30 days
4. Document your improvement plan with specific timelines and responsibilities

GUARDIAN
CLOUD SECURITY. REIMAGINED.

www.guardiancssp.com

It's time to close the gaps, from compliance documentation to comprehensive protection.
Get started with Guardian today.

To learn more, visit www.guardiancssp.com or contact us:
Steve Heinrich, Regional Sales Director | steve.heinrich@guardiancssp.com | 512-426-7580

Cybersecurity Assessment - 5 Critical Questions

5 Critical Security Areas Every Law Firm Should Evaluate

Questions about your assessment results?

Contact us for a confidential discussion about your specific cybersecurity needs and practical steps.

Email or call:
Steve Heinrich | Steve.Heinrich@guardiancssp.com | 512-426-7580
Visit Guardian online at www.guardiancssp.com.

Content developed with AI assistance and revised and reviewed by Guardian CSSP professionals.