Nasstar | FORTINET

Board-level questions for secure law firms

Playbook

2026

Exploring digital risk, client protection, and AI in legal environments

Technology plays a central role in fee-earner productivity, client confidentiality, and a firm's ability to maintain trust and secure future business.

In more mature organisations, digital risk is recognised as a business issue. Leadership teams work closely with IT and risk specialists to ensure that technology decisions are aligned with broader organisational priorities.

However, this level of integration is not yet consistent across the sector. In many firms, cyber risk remains primarily within the remit of IT. As environments become more interconnected, this approach is becoming increasingly difficult to sustain.

The following questions are designed to support leadership teams in assessing their current position, challenging assumptions, and identifying areas where greater control, visibility, and alignment may be required.

Ownership and accountability

Business implications

Where technology ownership is unclear, accountability becomes fragmented, which increases exposure to operational and reputational risk.

01 Who is responsible for technology risk across the firm?

02 Is there clear ownership for networking, security, and AI?

03 Are responsibilities between IT, risk, and leadership appropriately defined?

04 Who is accountable when technology impacts client confidentiality or service delivery?

05 Are critical systems and experimental tools (e.g., AI) governed with the same clarity as other core business functions?

Help along the way: A managed service provider specialising in secure networking can support the definition of governance models to help you clarify ownership, accountability, and escalation pathways across the organisation.

Access and control

Business implications

Inadequate access controls increase the likelihood of unauthorised data exposure, with direct implications for client confidentiality and trust.

01 Do we maintain appropriate control over access to systems and data?

02 Is there a clear understanding of who can access:

a. Case management systems

b. Document management platforms (e.g. iManage, NetDocuments)

c. Financial and billing systems

03 Are access rights aligned to roles and reviewed regularly?

04 How is access governed for remote users, third parties, and clients?

05 Are AI tools subject to the same access controls as other systems?

Help along the way: A specialist MSP can implement identity-led access frameworks so that access is controlled, monitored, and aligned with organisational policies.

Data exposure and client risk

Business implications

Unmanaged data exposure presents a direct risk to client confidentiality, with potential consequences for reputation and future business.

01 Where is sensitive or regulated data held, and who can access it?

02 Could systems or AI tools expose confidential information unintentionally?

03 Is there a clear understanding of how data moves across cloud environments, offices, and third parties?

04 Have legacy risks, such as excessive permissions or uncontrolled sharing, been addressed?

Help along the way: A managed service provider can help identify data exposure risks, improve visibility, and implement controls that reduce risk while supporting operational requirements.

Visibility and oversight

Business implications

Limited visibility of critical systems can delay incident response times and increase the impact of cyber attacks.

01 How quickly can issues be identified and investigated?

02 Are there gaps in visibility across remote access, cloud services, or third-party platforms?

03 Does reporting provide meaningful insight to non-technical stakeholders?

Help along the way: A specialist MSP can provide centralised monitoring and reporting. This will improve oversight and improve the accuracy of insights.

Resilience and continuity

Business implications

Disruption to core systems can directly affect revenue, productivity, and client service delivery.

01 How robust are the systems supporting fee earners and client services?

02 What is the operational impact of system disruption?

03 Are failover and recovery processes clearly defined and tested?

04 Can the firm continue to operate securely during an incident?

Help along the way: A managed service provider can design and manage resilient network architectures that ensure the continuity of service and rapid recovery when required.

Threat readiness and response

Business implications

Delayed detection and response can increase the scale and impact of security incidents, including reputational damage.

01 Are mechanisms in place to identify unusual behaviour or emerging threats?

02 How quickly can threats be contained and investigated?

03 Is there a clear understanding of potential impact across clients and systems?

Help along the way: A Modern MSP can provide continuous monitoring and structured incident response capabilities. This will reduce response times and the burden on internal IT teams.

Compliance, trust, and reputation

Business implications

Security posture is increasingly linked to client confidence, reputation, and the ability to secure new work.

01 Could we demonstrate and defend our approach to risk management?

02 Can we evidence how client data is protected across systems?

03 Are practices aligned with regulatory requirements such as GDPR?

04 Is there sufficient documentation to support decisions and controls?

05 How would clients assess the firm's approach to security?

Help along the way: A specialist MSP can support compliance through consistent controls, audit-ready reporting, and clear documentation.

AI risk and governance

Business implications

AI introduces new considerations around data access, governance, and risk, particularly in environments handling sensitive information.

01 Which AI tools are in use across the firm?

02 What level of access do these tools have to internal data?

03 Are governance frameworks in place for adoption, use, and oversight?

Help along the way: A managed service provider can support the development of governance frameworks and implement controls that enable secure AI adoption.

Enabling growth and innovation

Business implications

Technology capability is increasingly tied to competitive positioning and long-term growth.

01 Can new tools, including AI, be adopted without introducing unmanaged risk?

02 How easily can systems scale to support growth?

03 Are IT teams able to focus on strategic priorities?

04 Is technology enabling or constraining progress?

Help along the way: A managed service provider can help simplify environments, reduce operational burden, and create a foundation for secure innovation.

Connecting risk, resilience, and performance

Digital risk sits at the intersection of operational performance, client trust, and long-term strategy. Secure networking underpins the ability to manage this complexity.

The role of a specialist partner

Addressing these challenges requires a coordinated and well-informed approach. A managed service provider with expertise in secure networking can support law firms by:

- Protecting sensitive client data
- Reducing the risk of operational disruption
- Strengthening compliance and governance
- Enabling the secure adoption of new technologies

We'll ensure that technology aligns with how your firm operates, both now and in the future.

Ben Moorhouse

Business Development Director

Our Fortinet specialisations

FORTINET ENGAGE Account Specialization — SECURITY OPERATIONS

FORTINET ENGAGE Account Specialization — OPERATIONAL TECHNOLOGY

FORTINET ENGAGE Partner Specialization — SECURE NETWORKING FIREWALL

FORTINET ENGAGE Account Specialization — SASE

FORTINET ENGAGE Account Specialization — SD-WAN

FORTINET ENGAGE Account Specialization — SECURE CONNECTIVITY LAN

nasstar.com

0345 003 0000

salesenquiries@nasstar.com

Follow us