Here are five key tactics that IT leaders at law firms should be using to mitigate mobile security risks while still giving their attorneys the productivity tools they need.

**Five Mobile Security Tactics for Legal Firms**

**A Legal Defense**

**Smartphones can help law firm employees stay connected, respond faster, and access legal briefs and other client data on-the-go. But that data is highly sensitive, and a lost or hacked device can have massive repercussions on a law firm's reputation and revenue.**

**Security Awareness Training**

Frequent training helps raise awareness of mobile security risks, ensuring policies and procedures are in place to protect client data.

**Favor Corporate-issued Devices**

A corporate-issued approach allows easier mobile management and ensures that all devices that access client data meet key security criteria.

**Enterprise Mobility Management Tools Are Essential**

71% of law firms are already using MDM solutions; those that aren't are putting their firms at risk.

Effective MDM solutions provide the ability to:
- Remotely lock or wipe lost devices
- Keep track of devices across the firm
- Prevent access to risky apps and websites

**Deploy a “Container” to Separate Personal and Professional Data**

Containerization solutions create a separate, encrypted area on the device that is insulated from personal web-surfing and app use.

**Manage Apps Strategically**

25% of apps include at least one security flaw. Use enterprise application management tools like those available in Google Play for Work to:
- Provision core legal and productivity apps on all devices, and blacklist risky apps
- Deploy custom-built or licensed applications to the specific user groups who need them

Find out more about Samsung's secure mobile solutions for legal professionals at: samsung.com/legal