THREATS LIBRARY

JULITH GmbH
Awareness-as-a-Service

Mobile & BYOD - when the private phone carries company data

Smartphones are now work devices - but rarely managed like laptops. We show which risks arise from BYOD setups and where MDM, app containerisation, and training usefully work together.

min read: 7 min **Updated:** 14 March 2026 **Risk:** Medium risk
Source: awareness-as-a-service.com/en/resources/threats/mobile-byod

What is BYOD and why is it a security issue?

BYOD (Bring Your Own Device) is the practice of using personal smartphones, tablets, or laptops for work purposes. What is convenient for employees creates significant security and privacy challenges for IT: personal devices are not subject to corporate patch management, no MDM policies enforce device encryption, and the employer has little room to act in the event of a loss or security incident.

In many organizations, BYOD is not a deliberate decision - it simply happens: employees set up their work email on their personal phone, use Microsoft Teams or Slack on a personal iPad, and access company documents from the family tablet. The boundary between personal and professional blurs.

The problem is not BYOD itself, but BYOD without governance. With clear policies, minimum technical requirements, and training, the risk can be reduced to an acceptable level.

At a glance

01

Personal devices are rarely securely configured

Outdated OS versions, disabled device lock, insecure backup cloud - on personal devices, security configurations that are standard in enterprise environments are often absent.

02

Data separation is solvable

Container solutions (Android Work Profile, Apple MDM enrollment) enable a technical separation of personal and professional areas - without full device control.

03

Loss without reporting is an underestimated risk

A lost phone with corporate email, not reported immediately because the employee "might find it", can be compromised for days.

How to recognise BYOD risks

Unencrypted backup cloud
Corporate emails and documents automatically backed up to a personal iCloud, Google Drive, or Dropbox - without IT or compliance knowing.

Side-loaded apps
Apps installed outside official app stores (APK sideloading on Android) are a frequent malware vector.

No PIN or biometric lock
Devices without a screen lock, on which corporate apps are running - anyone who picks up the device has access.

Family accounts on shared devices
A tablet shared by a partner and children, on which corporate apps are also installed.

Device loss not reported immediately
Employees who notice a device with corporate access is missing and "wait to see if it turns up" before informing IT.

Very old OS versions
Smartphones running iOS or Android versions several years old, no longer receiving security updates, but still used for work.

How to protect yourself

For employees

- **Device lock always active:** At minimum a PIN, ideally biometric lock (Face ID, fingerprint) with a maximum 5-minute lock timeout.
- **Keep OS and apps up to date:** Install security updates promptly - if in doubt, enable automatic updates.
- **Report device loss immediately** - do not wait. IT can trigger a remote wipe and remove corporate data from your device without deleting personal photos or contacts (with an MDM container solution).
- **Install work apps only from official stores;** no APKs from unknown sources.
- **Separate work email configuration** - do not mix personal and work email accounts in the same app.

For administrators

- **Formalise the BYOD policy:** Written agreement with minimum requirements (OS version, device lock, encryption, no jailbreak/root).
- **MDM container solutions (Android Enterprise / Apple Business Manager):** Separation of personal and corporate areas on the same device; remote wipe only of the corporate container is possible.
- **Conditional Access:** Corporate services (Microsoft 365, Google Workspace) accessible only on devices that meet minimum requirements (device compliance check).
- **Mobile Threat Defence (MTD):** Detects jailbreaks, malicious apps, and insecure network connections on personal devices.
- **Maintain a BYOD inventory:** Which personal devices have access to corporate data? Without an inventory, there is no risk management.

Real cases

CASE 01 · LAW FIRM · DE · Q1/2026

A lawyer used his personal smartphone for client communications. The device was configured with iCloud backup, which automatically synchronised client matter data. After a breach of the lawyer's iCloud account (through phishing), attackers accessed confidential client files.

Damage: breach of professional confidentiality, loss of mandate · **Detection:** the lawyer himself, after suspicious iCloud activity · **Lesson:** Client communications on uncontrolled personal devices is not GDPR-compliant. MDM container or a company device would have been required.

CASE 02 · MANUFACTURING COMPANY · CH · Q3/2025

A production manager lost his personal smartphone, on which he had configured Teams and SAP access. He waited two days to see whether it would turn up. In that window, someone logged into internal systems using stored credentials.

Damage: unauthorised access to production plans, access active for 48 hours · **Detection:** SIEM anomaly alert on login geography · **Lesson:** Remote wipe triggers and an immediate reporting requirement for device loss must be part of the BYOD policy.

What to do if it happens?

THE FIRST 15 MINUTES

1. **Inform IT immediately** for device loss or suspected compromise - not the next day.
2. **Request remote wipe** of the corporate container (with MDM: only the work area is wiped).
3. **Change credentials for all work apps** that were stored on the device.
4. **Invalidate active sessions** for Microsoft 365, Teams, VPN, and other services.
5. **Remotely deregister corporate apps** where possible (MDM deregistration).
6. **File a police report** for theft - for insurance and documentation purposes.

Frequently asked questions

Can employers control personal devices?

With an MDM solution and a BYOD agreement, yes - within limits. Without written consent and restriction to the corporate container, extensive control is legally problematic. Container solutions are the pragmatic compromise: IT controls only the corporate area, not the personal device.

What is the difference between BYOD and COPE?

COPE (Corporate-Owned, Personally Enabled) means the company provides the device but permits personal use. BYOD is the reverse: a personal device used for work. COPE gives IT more control; BYOD is more convenient for employees.

What happens to personal data during a remote wipe?

With a proper MDM container deployment, only the corporate area is wiped - personal photos, contacts, and apps are untouched. A full device wipe (without a container) deletes everything. This should be clearly regulated in the BYOD agreement.

Related topics

BYOD risks intensify while travelling - the same device on an insecure hotel network is a compounded risk. Uncontrolled apps on personal devices are also a shadow IT entry point.