Cybersecurity Self-Assessment

CyberScore: 

Report generated on: **08/11/2026 20:16**

> This report is simply a self-assessment of your IT security level, based solely on your answers to the questionnaire designed by Oxydian's experts. It does not in any way constitute an in-depth technical audit. While it gives you an initial overview of your cybersecurity strengths and weaknesses, it is no substitute for a rigorous analysis of your infrastructure and systems. To go further and benefit from a full technical audit, please feel free to contact us:
>
> contact@oxydian.fr

Summary:

Your security level shows significant weaknesses that require immediate attention. The risk of certain vulnerabilities being exploited is high, which could compromise the overall security of your organisation. We strongly recommend implementing corrective measures and suggest specialist support to carry out an in-depth audit.

Scores by category (40.0%)

Passwords

Data Security



Monitoring and Detection



Internal Security



External Security



Security Management



Risk Identification



Physical Security



Personalised action plan:

This action plan is based on the results of your assessment. We recommend that you follow this advice to improve your IT security.

Secure password storage
Make sure all passwords are stored in a secure password manager rather than on unsecured media.

Use antivirus software
Make sure all your servers and computers are equipped with up-to-date antivirus software to detect and block threats.

Replace outdated computers
Replace or migrate outdated computers (Windows XP, Vista, 7, 8 or Windows Server 2003 / 2008 / 2012) to reduce the risk of unpatched vulnerabilities.

Separate user and administrator rights
This practice involves assigning separate accounts for day-to-day tasks and administrative tasks. It considerably reduces the risk of a security compromise by restricting elevated privileges to the specific operations that require administrative access.

Implement a password policy
Put a robust password policy in place to ensure that passwords are secure, complex and renewed regularly.

Protect email with 2FA
Enable two-factor authentication (2FA) on all of the company's email accounts (Microsoft 365, Google Workspace, etc.). Email compromise is the most common attack vector targeting SMEs, and 2FA blocks the vast majority of these attacks.

Regular password analysis
Have your passwords analysed regularly by a professional or your IT department to detect weak and reused passwords and strengthen security.

Implement disk encryption
We strongly recommend enabling disk encryption on all PCs and servers, using solutions such as BitLocker for Windows or LUKS for Linux, to protect your sensitive data against unauthorised access.

Backup restore testing
Schedule regular restore tests (at least once a quarter) to check that your backups are genuinely usable and to measure the time needed to resume your operations.

Map external assets
Regularly update and complete the map of your internet-facing assets to improve security management.

Implement 2FA for the VPN
Enable two-factor authentication (2FA) for all VPN access to strengthen the security of remote connections.

Incident response procedure
Formalise an incident response procedure: first steps to take, a list of emergency contacts (specialist provider, insurer, the data protection authority in the event of a data breach) and internal roles. Test it at least once a year through a tabletop exercise.

Implement two-factor authentication
Enable two-factor authentication (2FA) on all your critical accounts and services to add an extra layer of security.

Backup redundancy
We strongly recommend storing your backups in several separate locations to reduce the risk of data loss in the event of a disaster.

Move to an EDR
Replace or supplement your traditional antivirus with an EDR (Endpoint Detection and Response) solution, capable of detecting malicious behaviour and isolating compromised computers in the face of modern attacks such as ransomware.

Centralise logs
Centralise the logs of your servers and critical devices on dedicated storage and retain them for several months (6 to 12 months recommended). This allows incidents to be detected and analysed even if the attacker erases local traces.

Map internal assets
Regularly update and complete the map of your internal assets to improve security management.

Wi-Fi network segmentation
Set up several Wi-Fi networks to separate public and internal access, strengthening security while still offering public Wi-Fi for internet access only.

Implement an external update policy
Adopt a strict update policy for all your external assets to minimise the risks associated with vulnerabilities.

Implement an IT acceptable use policy
Make sure all employees sign an IT acceptable use policy setting out security rules and good practices, with an emphasis on protecting personal data to meet GDPR requirements.

Regular phishing simulations
Run phishing simulation campaigns at least once a year to measure your employees' reflexes in real-life conditions and focus awareness training on the weaknesses identified.

Control third-party access
Control your providers' access: dedicated named accounts, rights limited to what is strictly needed, systematic deactivation at the end of each intervention or contract, and logging of connections.

Server room access control
Implement strict access control for the server room to prevent unauthorised tampering.

Implement an onboarding/offboarding procedure
Make sure you define a clear procedure for staff joining and leaving, including the removal of accounts and access, to protect the company against security risks.

Key:

INFORMATION

No overall risk, these are simply observations raised during the audit.

MINOR

Low overall risk that does not require significant action.

MODERATE

Moderate overall risk that requires action in the medium term.

MAJOR

Major overall risk that requires action in the short term.

CRITICAL

Critical overall risk that requires immediate action.