

EXECUTIVE BRIEF

Security Assessment - ABCD Ltd

OVERALL RISK RATING: CRITICAL

Executive Summary

ABCD Ltd engaged an independent IT security audit of its network to assess its vulnerability to attack. Our red team launched a realistic attack against the company's web server, corporate network and user workstations using the same methods as those likely to be used by criminals who target UK retailers.

We discovered that an intruder could gain full control of the company network and access all customer information in just two hours from initial network contact, without raising any alarms. This poses a serious threat to the organisation.

Key Findings

CRITICAL: The company site has software with a security defect that is more than 14 years old. This enabled our team to have complete administrative power to the web server in less than two minutes.

CRITICAL: There are multiple staff accounts that have weak passwords that can be easily guessed i.e. Password123 and Summer2025!. The passwords, together with the lack of multi-factor authentication, allowed having immediate access to the most sensitive systems of the company.

CRITICAL: 10 customers personal data (names, email addresses, home addresses) were accessed and downloaded via an employee workstation. This information was stored in the unencrypted form and there was no monitoring of access.

HIGH: There are no security monitoring tools deployed in the network. The main server of the company has no intrusion detection system, security event logging and no protection of the end points. The whole attack went on without raising a single alarm.

Business Impact

If this attack were carried out by a real criminal group, the consequences for ABCD Ltd would be severe:

- **Regulatory fines:** Fines imposed by UK GDPR on data breaches involving the personal data of customers may include up to 4% of annual global turnover or 17.5 million, whichever is higher.
- **Reputational damage:** Customer trust and the brand image would be seriously hurt by publicity of a data breach with customer addresses and personal information.
- **Operational disruption:** Due to full access to the domain controller, an attacker may lockout all the staff, encrypt all files (ransomware), or even shut down the business activity.
- **Legal liability:** Affected customers might take legal action against the company on the basis of the Data Protection Act 2018 in case they have not sufficiently safeguarded their personal data.
- **Notification requirements:** The ICO should be notified of a qualifying data breach within 72 hours of its awareness. Even affected persons should be informed promptly.

Prioritised Remediation Recommendations

Priority	Recommendation	Estimated Cost	Timeframe
CRITICAL	Upgrade all of the services that face the internet. Get rid of or upgrade the old web server software as soon as possible.	Low (£1-5K)	1-2 weeks
CRITICAL	Implement a password policy: minimum 14-character passwords with complexity. Change all existing passwords.	Low (£0-1K)	1 week
CRITICAL	Implement multi-factor authentication (MFA) that is phishing resistant on every staff account, and administrators in particular.	Medium (£5-15K)	2-4 weeks
HIGH	Install Endpoint Detection and Response (EDR) software on every server and workstation and identify malicious activity.	Medium (£15-30K/yr)	1-2 months
HIGH	Use network segmentation to separate the web server and internal corporate network and sensitive data.	Medium-High (£20-50K)	2-3 months
HIGH	Encrypt all sensitive data stored, especially customer database, and payroll information found on employee workstations.	Low (£2-5K)	2-4 weeks
MEDIUM	Implement a Security Information and Event Management (SIEM) system, with monitoring policies on Active Directory attacks.	High (£40-80K/yr)	3-6 months
MEDIUM	Install a Data Loss Prevention (DLP) system to identify and prevent unauthorised movement of sensitive files.	Medium (£20-40K/yr)	3-6 months
MEDIUM	Periodically, as every quarter, perform vulnerability testing and penetration testing..	Medium (£15-25K/yr)	Ongoing

Conclusion

The security assessment found out that the current IT systems of ABCD Ltd have key vulnerabilities that can enable an average-skilled attacker to completely compromise the entire corporate network and gain all the customer data in a few hours. The lack of fundamental security measures - patching, strong passwords, multi-factor authentication and security monitoring - implies that such an attack would completely remain unnoticed.

We highly suggest that the Board consider the three Critical-priority items as urgent business issues that need to be acted upon in the next two weeks. The approximate price to be paid to deal with the three most severe vulnerabilities is less than £20,000 - a drop in the ocean compared to the regulatory penalties, legal expenses, and reputational losses in case of a real data breach.

Report prepared by: Sanjay, Red Team Specialist

Date: May 2026

Classification: Confidential - Board of Directors Only