GLOBE2

Executive Briefing

KPN Logistics Group Ransomware Breach — Lessons for Every Business

In June 2023, KPN Logistics Group — a £95M turnover logistics company with 900+ employees — was hit by a devastating ransomware attack. Despite ISO 27001 certification, cyber insurance, and previous phishing awareness training, the company collapsed within three months. Over 730 jobs were lost, and no ransom was paid.

Impact	Details
Employees affected	730 job losses
Business closure	September 2023
Ransom demand	$2M – $5M
Systems compromised	Core transport & warehouse platforms
Backups compromised	Yes — including offsite copies

Key Lessons for Business Leaders

• Cybersecurity must be a **board-level priority** — IT risk is business risk.
• **Test, don't assume** — disaster recovery and backups must be stress-tested regularly.
• **Enforce MFA** and secure password policies across all systems.
• Benchmark your **MSP's capabilities** and demand evidence of security controls.
• Prepare for **when**, not **if** — ransomware threats are growing in sophistication.

5-Step Cyber Resilience Checklist

✓ Put cybersecurity on every **board meeting agenda**.
✓ **Test** disaster recovery and business continuity plans now.
✓ **Enforce MFA** and secure all endpoints.
✓ Schedule **independent security assessments** and penetration testing.
✓ Work closely with **MSPs, insurers, and leadership teams** to align strategy.

Final Takeaway: "If cybersecurity isn't on your agenda, you're inviting trouble." The KPN Logistics breach shows how a lack of preparedness can be catastrophic.