KPN Logistics Ransomware Overview

Notes taken from interview with KPN Logistics former Director, Paul Abbott

---

Overview

- **Company**: KPN Logistics Group
- **Turnover**: £95M | **Employees**: 900+
- **Subsidiaries**: Knights of Old (158 yrs), Nelson Distribution, Steve Port Transport, Merlin Supply Chain Solutions.
- Privately owned, strong in its sector, but not a household name.

The Attack

- **Date**: June 2023
- **Type**: Ransomware
- **Initial Signs**: Systems slowed overnight → IT rebooted → ransom note appeared next day.
- **Cause**: Likely **password compromise** from an employee working remotely, no **2FA** on all systems.

Immediate Impact

- Complete loss of access to critical systems.
- Severe **operational disruption** and move to **manual, paper-based processes** to keep trucks moving.
- Communication breakdown: switched to temporary Gmail accounts.
- High stress, panic, and uncertainty.
- **Costs skyrocketed**:
    - Efficiency losses.
    - Cybersecurity experts and first responders.
    - Escalating operational expenses.

GLOBE2

Business Collapse

- Hackers demanded **$2–5M** ransom (unaffordable).
- Despite backups, hackers accessed offsite copies too.
- Insurance supported rebuilding systems but could not offset wider financial damage.
- Company **closed September 2023**:
    - **730 job losses**.
    - Zero ransom paid, hackers gained nothing.

Role of Insurance

- Connected KPN with **expert negotiators** familiar with the attacker group.
- Advised on expectations and likelihood of hackers honouring promises.
- Guided decision **not to negotiate** due to ransom size.
- Provided legal, technical, and first-response support.

Key Lessons

1. Cybersecurity Must Be a Board-Level Priority

- IT was treated as a cost centre, not a strategic risk.
- The board lacked knowledge to challenge MSPs or make informed decisions.
- Analogy: **Health & Safety is always at the top of the board agenda — cybersecurity should be treated the same way**.

2. Disaster Recovery & Business Continuity

- Plans existed but were **inadequate and untested**.
- No strategy for operating without the main site.
- Backups failed because attackers compromised them too.
- New infrastructure post-breach is **cheaper and more secure** — knowledge gap, not cost, was the real issue.

3. MSP Relationship Failures

- Long-standing IT provider but **insufficient skills and proactivity**.
- Assumptions made about protections that didn't exist.
- Businesses must **benchmark providers** and demand evidence of security measures.

4. Evolving Threat Landscape

- Ransomware attacks are **increasingly sophisticated**.
- Yesterday's defences may already be obsolete.
- Cyber insurance helps, but **cannot prevent disruption or reputational damage**.

5. Actionable Recommendations

- **Regularly test disaster recovery** and incident response plans.
- Enforce **multi-factor authentication (MFA)** across all systems.
- Use **SOC (Security Operations Centre) monitoring** for early threat detection.
- Ensure **board-level cybersecurity education** to make informed investment decisions.
- Build **trust-based relationships** with MSPs and request independent security assessments.
- Include **supply chain resilience** in risk planning — single points of failure amplify impact.

Big Takeaway

"If cybersecurity isn't on your board agenda and regularly tested, you're inviting trouble. The threat is growing, and naivety can be catastrophic."
