**Cyber Risk Planning Help Sheet: 21 Days to Bankruptcy Prevention**

## The Reality Check

- **21 days** = Average downtime after a cyberattack
- **14 days** = How long many businesses can survive without operations
- **Result**: You could go bankrupt before recovery is complete, even with backups

## Who's At Risk?

**Mid-sized companies are the sweet spot for attackers:**

- Fast growth but IT security hasn't kept pace
- Often uninsured or facing rejected claims
- Leadership focused on revenue, not risk

## The Insurance Problem

**Insurers are pulling back hard:**

- Requiring cyber audits before coverage
- Demanding evidence of robust IT systems
- Rejecting claims due to "inadequate security"
- Steep premiums or complete refusal for unprotected firms

*"Most of the time, when a company gets hacked, the insurance company says their security has not been sufficient enough to cover the risk, so they won't pay out."*

## Immediate Action Plan

**Step 1: Conduct an IT Security Audit**

### External Assessment:

- Penetration testing on websites
- Test customer portals and public-facing systems
- Identify open ports and vulnerabilities

### Internal Assessment:

- Password rotation policies
- Access logs and user permissions
- Server room physical security
- Documentation gaps

## Step 2: Develop Your Recovery Strategy

### Business Impact Analysis (BIA):

- Identify critical systems and processes
- Calculate daily revenue loss during downtime
- Map dependencies between systems

### Emergency Recovery Programme (ERP):

- Prioritise which systems to restore first
- Create step-by-step recovery procedures
- Test your backup and recovery processes

## Step 3: Reduce Recovery Time

### Consider Mirror Servers:

- Can reduce recovery from 21 days to 1-2 days
- Significant investment but could save your business
- "Recovery in 1-2 days compared to 21 days... is a completely different answer"

## Common Vulnerabilities to Address

- Open network ports
- Weak credential policies
- Missing system documentation
- Unpatched software and systems
- Poor access controls
- Inadequate backup testing

## The Bottom Line

**Don't wait for an incident to plan.**

Waiting until after an attack to develop your cyber risk strategy is like buying fire insurance while the building burns. The time to act is now, before you become another statistic.

## Next Steps

1. Schedule an IT security audit within the next 30 days
2. Review your current insurance coverage and requirements
3. Begin developing your Business Impact Analysis
4. Test your backup and recovery procedures
5. Consider investing in mirror server infrastructure

**Remember:** It's not about IF you'll be attacked, it's about WHEN—and whether you'll survive the aftermath.