

THE MANUFACTURING DISRUPTION DECISION KIT

A practical 20-minute exercise for operations, IT and finance

An Assured Digital resource | October 2026

Why this exists: A technology outage is rarely just a technology problem. It can delay a customer order, spoil material, interrupt cash collection or expose information that is difficult to replace. This kit helps a manufacturing team examine **one important process**, record what is actually known and decide what is worth testing next.

You can use this with your existing IT provider. This is not a cybersecurity assessment, an audit, a forecast or a claim that your organisation has any particular weakness. Write **Unknown** wherever evidence is missing rather than guessing.

How to run it: Invite one operations owner, one IT/contact for your IT provider and, where useful, someone from finance. Allow 20 minutes to identify one workflow and its dependencies. A longer financial review can follow. Never add trade secrets, personal data or access credentials to a shared worksheet.

WORKSHEET 1 | CHOOSE ONE BUSINESS-CRITICAL PROCESS

Selected process: _____

Business owner: _____ IT owner/provider: _____

Date and next review: _____ Key customer or delivery deadline: _____

Why it matters (one sentence): _____

Question	Our answer / evidence
Which customer outcome does the process enable?	
What normal volume or value depends on it?	
What would people notice first if it stopped?	
How long can it stop before a material business consequence?	
Who makes the decision to use a fallback?	
When was end-to-end continuity last demonstrated?	

Choose one starting point: Customer orders / Production scheduling / Materials and stock / Quality records / Dispatch and labelling / Supplier or customer integration / Technical information needed for production.

Trace the dependencies, not just the software

Use 4–6 rows. Ask: *What must work for this process to complete successfully?* List identity, network, applications, suppliers and people where relevant.

Dependency	Internal owner or supplier	Safe fallback available?	Last tested / evidence	Unresolved question
1.				
2.				
3.				
4.				
5.				
6.				

An important distinction: The fact that a dependency has not been tested does not prove it is insecure. It tells you where assurance is missing.

WORKSHEET 2 | THE 4 / 24 / 72-HOUR INTERRUPTION DRILL

Scenario: It is 09:00 on a normal working day. The selected process cannot complete because one essential business system or external service is unavailable. Staff and physical equipment may be ready, but the information or service is not. You do not yet know the cause.

Decision point	What must the team know or decide?	Owner	Actual action / unresolved issue
First 4 hours	Which jobs or orders are affected? Is a safe workaround possible? Who is incident lead?		
At 24 hours	Which customer commitments slip? Who communicates with customers/suppliers? What costs need authorisation?		
At 72 hours	Which production, staffing, cash and stock decisions are urgent? Who can approve them?		
After restoration	How will manual entries, stock, invoices and dispatches be reconciled without duplicates?		

A useful test order

Pick an ordinary customer order. Record whether the team can **receive it → check stock → pick or produce → label → release or dispatch → invoice → reconcile** under the agreed fallback. Note any stage that cannot be completed or evidenced. If a stage is irrelevant to your business, replace it with an appropriate real step.

Customer communication owner: _____

Escalation contact for critical supplier: _____

Manual records kept where: _____

Maximum acceptable interruption agreed by: _____

WORKSHEET 3 | WHAT COULD THE INTERRUPTION COST?

Model a scenario, not the probability of an attack

Use business figures only where the finance owner is comfortable sharing them internally. If figures are uncertain, record a range and the evidence you need. These calculations are **illustrative financial scenarios**, not an expected cyber-loss estimate.

Input	Explanation	Your figure
A. Affected customer orders/output per day (£)	Only the value linked to the selected process, not all turnover by default	£
B. Contribution margin (%)	Revenue less variable costs, as agreed with finance	%
C. Share of orders/output permanently lost (%)	Exclude sales that will be fulfilled after recovery	%
D. Interruption (days)	Consider 0.5, 1 or 3 days; choose a credible scenario	days
E. Additional incremental costs (£)	Evidenced scrap, emergency freight, extra labour and response costs not already counted	£
F. Savings / mitigations / overlap (£)	Avoided variable costs and items already included; prevent double counting	£

Indicative lost contribution = $A \times (B / 100) \times (C / 100) \times D$.

Illustrative total = **indicative lost contribution** + E – F.

Worked example (not a sector benchmark): £240,000 of affected orders per day × 32% contribution × 50% unrecoverable × two days = **£76,800** in lost contribution. If separately evidenced extra costs are £36,000 and there are no adjustments, the preliminary illustration is **£112,800**. The real figure may be much lower or higher depending on recovery, insurance, stock accounting, mitigation and whether orders are merely delayed.

Important exposures that may NOT belong in the arithmetic

Exposure	What evidence would be required before assigning £ value?	Owner
Delayed cash receipts and finance costs	Payment schedule, borrowing or working-capital effect	
Contract penalties or customer concessions	Signed contract and actual trigger	
Future lost orders or customer	Commercial evidence and	

Exposure	What evidence would be required before assigning £ value?	Owner
confidence	scenario assumptions	
Confidential design, know-how or bid disclosed	Asset-specific assessment, contractual and legal advice	
Insurance recovery or exclusions	Actual policy terms and insurer assessment	
Ransom demand or specialist response	Incident-specific professional guidance, not a standard assumption	

Finance owner's conclusion: Our credible exposure is £_____ to £_____, subject to the assumptions:
_____.

WORKSHEET 4 | WHAT PROTECTION AND RECOVERY HAVE WE ACTUALLY PROVED?

For the one selected process, choose **Tested and evidenced** / **Documented only** / **Unknown**, and record the proof rather than a vague yes/no.

Question	Status	Evidence or date	Next action / owner
Is there a business owner and agreed tolerable interruption?			
Are the critical systems and supplier dependencies recorded?			
Have recovery tests demonstrated the entire business outcome?			
Are backup, access and network dependencies understood?			
Has the manual fallback been exercised safely?			
Can manual records be reconciled after restoration?			
Are supplier escalation and customer communications assigned?			
Are incident and spending decisions assigned at 4, 24 and 72 hours?			

Do not turn the number of 'Unknown' entries into a cyber-risk score. These entries identify where more evidence or a practical test could improve confidence.

WORKSHEET 5 | IP & SUPPLIER ACCESS: ONE VALUABLE INFORMATION ASSET

Do not paste or upload the actual information asset, passwords, account names or confidential content. Give it a generic label such as *Current drawings for Product Group A*.

Generic asset name: _____

Why it matters (products, contracts, competitive advantage): _____

Business information owner: _____

Known storage locations (systems only): _____

Who legitimately needs access: Internal teams / Contractors / Suppliers / Customers / Other.

Access or information-control question	Tested / documented / unknown	Owner / evidence and next check
Can we identify current internal and external access?		
Can we list active external sharing links or supplier accounts?		
Who approves changes, and how are privileges reviewed?		
Can access be withdrawn when someone leaves or a project ends?		
Do we understand whether local copies/downloads are permitted?		
Do contracts address confidentiality, onward sharing and retention?		
Can we investigate suspected disclosure or altered file versions?		
Are availability, integrity and confidentiality all addressed separately?		

Three immediate checks:

1. Action _____ Owner _____ Deadline _____ Evidence _____
2. Action _____ Owner _____ Deadline _____ Evidence _____
3. Action _____ Owner _____ Deadline _____ Evidence _____

Remember: Restoring a backup does not reverse a disclosure. An access review and a proven recovery plan address different problems.

WORKSHEET 6 | ONE-PAGE LEADERSHIP DECISION

Manufacturing interruption / information exposure decision brief

Business-critical process or information collection: _____

Business owner and date: _____

Why it matters commercially: _____

Customer, production or contract deadline at stake: _____

Known technical, supplier and people dependencies: _____

What we've actually tested: _____

What we have documented but not tested: _____

What remains unknown: _____

Four-hour outcome: _____ 24-hour outcome: _____

72-hour outcome: _____ Recovery/reconciliation: _____

Illustrative direct financial impact: £_____ to £_____

Assumptions, exclusions and hard-to-price risks: _____

The three decisions we need to make

Priority	Specific decision or test	Responsible person	Due date	Evidence needed
1				
2				
3				

Recommended next step (tick one): Test existing fallback / Improve process ownership / Review supplier dependency / Verify Microsoft, infrastructure or recovery control / Obtain specialist input / Accept and monitor with documented rationale.

Review decision with: Operations / IT or provider / Finance / Senior leader.

WHAT THE CASES TELL US, WITHOUT OVERCLAIMING

- **JLR, 2025:** JLR disclosed £196m in cyber-related costs for its quarter ending September 2025. Its production restart was phased. [JLR report](#).
- **Wider JLR supply chain, 2025:** Cyber Monitoring Centre estimated £1.9bn UK-wide impact across more than 5,000 organisations. This includes JLR and suppliers and must not be added to the £196m. It is a modelled estimate. [CMC](#).
- **Carpentryright, 2024:** PwC reported an April cyberattack that prevented trading for a period as one of several pressures preceding administration. [PwC](#).

- **KNP Logistics, 2023:** UK government cites a ransomware attack that KNP blamed for insolvency, with over **700 jobs lost**. [UK government](#).
- **Manufacturing supply chain, 2026:** Among manufacturers affected by cyberattacks on suppliers, **31%** reported delays to customer deliveries, according to Make UK. [Make UK](#).
- **IP and knowledge assets, 2024:** Government-commissioned research estimated **£1bn to £8.5bn** of UK-wide economic loss from cyber-related IP and knowledge-asset theft. Not a figure for your company. [GOV.UK](#).

The point: News stories establish why the subject matters. **Your evidence and your own commercial assumptions determine what needs doing.**

About Assured Digital: We support organisations with business IT, Microsoft security and information governance, connectivity and recovery. A defined finding can be discussed with Matthew at Assured Digital without any assumption that you need to change your existing IT provider. This resource makes no promise of an audit, assurance opinion, restoration guarantee, specific solution or industrial-control remediation.