Preptorum

FAILURE SCENARIOS

EXAMPLE PACK: PELLBROOK & MARR
DOCUMENT 03
FICTIONAL · NOT A REAL COMPANY

Pellbrook & Marr · Continuity pack document 03

> **FICTIONAL EXAMPLE CONTENT – Pellbrook & Marr is not a real company.** The scenarios are generic examples. AWS, Azure and Microsoft are named only as platforms. No payment brands or providers are named. A real retailer replaces the details with its own systems and plans.

How to use this document: find the scenario that fits, then work through the five headings in order: signs, first actions, what still works, workarounds, and when to stand down. If tills, online orders or the warehouse are affected in any scenario, run the first-hour runbook (document 02) at the same time.

SCENARIO A: PEAK-SEASON CYBER ATTACK (LEAD SCENARIO)

In the weeks before Christmas, attackers get into the company network. Tills, the online store, order management and the WMS go down together or one after another.

Signs

- Tills freeze, show strange messages, or refuse to start.
- The online store or order management stops working; ransom notes or unusual account activity appear.
- The warehouse cannot open pick lists.
- Alerts from monitoring tools, or a warning from a provider or partner.

First actions

1. Report it at once to the Technology On-Call Lead and the cyber response lead by phone.
2. Do not switch off, wipe or reconnect affected machines unless the cyber response lead says so.
3. Incident Lead sets stores to **Restricted** and starts document 02.
4. Move all incident talk to the out-of-band bridge. Assume company email and Teams may be read by the attacker.
5. Data Protection Lead starts the breach assessment under our own procedures; involve legal counsel.

What still works

- The Preptorum drive, with price lists, rotas, contact sheets and templates, because it is not connected to the network. Treat any file copied to it after the suspected start time with care.
- Cash, paper sales books and, if your terminals and provider allow it, offline card payments.
- Store phones and personal mobiles.

Workarounds

- Trade on cash and offline card (document 02, section 4).
- Pause online orders and click-and-collect (document 02, section 5).
- Pick on paper in the warehouse (document 02, section 6).
- Confirm every instruction by calling back on a known number from the contact sheet, never one given in an email or message.
- Pause supplier payments and changes to bank details unless confirmed by phone and approved by two people.

Stand down when the cyber response lead confirms systems are clean and restored from trusted backups, credentials have been reset, paper records have been entered, and customers, staff and regulators have been told what they need to know under our procedures.

SCENARIO B: TILL OR PAYMENT NETWORK OUTAGE

Tills or card terminals cannot reach the payment provider, but there is no sign of an attack.

Signs

- Card payments decline or time out in many stores at once.
- Tills work but cannot complete card sales.
- The payment provider's status page or helpline reports a problem.

First actions

1. Store Managers report to their Regional Manager; Store Operations confirms how many stores are affected.
2. Incident Lead decides whether to set stores to **Restricted**.
3. Finance Duty Lead confirms with the payment provider whether offline card payments are allowed and within what limits.

What still works

- Cash sales on the tills, if the tills themselves work.
- The online store, if it uses a different payment route.

Workarounds

- Cash, and offline card within the provider's limits (document 02, section 4).
- Signs at the door and payment points so customers know before they queue.

Stand down when card payments work normally in every store, offline payments have been processed, and stores have been told.

SCENARIO C: AZURE OR MICROSOFT 365 OUTAGE

Teams, Outlook and the intranet are down, and staff may not be able to sign in with company accounts.

Why this matters now: on 12 November 2026 a widespread Microsoft 365 outage disrupted Outlook, Teams and other services for many organisations for about a day (dated sources in SOURCES.md). Outages like this are rare, but when they happen, the plan needs to be somewhere other than the system that has stopped.

Signs

- Outlook will not connect; Teams shows errors; SharePoint and the intranet will not load.
- Store managers cannot open the rota or store messages.
- The Microsoft 365 or Azure status pages, or news reports, describe a wider outage.

First actions

1. Incident Lead opens the out-of-band bridge (document 04, section 3) and sends the first SMS to stores.
2. Technology On-Call Lead checks whether tills, the online store or the WMS depend on company sign-in. If they do, start document 02.
3. Do not sign out of any working session; it may not come back.

What still works

- Tills and card terminals, if they do not depend on company sign-in.
- The online store on AWS.
- Store phones and personal mobiles.

Workarounds

- Rotas and shift messages by SMS and through Regional Managers (document 02, section 7).
- Use the contact sheets on the drive, not the address book.

Stand down when sign-in, email, Teams and the intranet work across head office, stores and the warehouse, and decisions made off-system have been written into the normal records.

SCENARIO D: AWS REGION OUTAGE

The online store and order management run in a primary AWS region, with a standby in a second region.

Signs

- The online store will not load, or checkout fails.
- Order management and click-and-collect lists stop updating.
- Technology alerts about the primary region; the AWS Health Dashboard reports a problem.

First actions

1. Online and Customer Service Lead puts up the holding message if the store can still show one.
2. Technology On-Call Lead confirms whether the fault is AWS-wide, regional, or ours.

3. If regional and not fixed within the agreed decision window (example: 30 minutes), the Incident Lead decides whether to fail over to the second region.

What still works

- Stores, tills and card terminals.
- Email, Teams and the intranet.
- The warehouse, if the WMS does not depend on the same region.

Workarounds

- Pause click-and-collect bookings; hand over parcels already in store from the collection list (document 02, section 5).
- After failover, check the standby holds the latest orders before reopening.

Stand down when the online store and order management run normally in either region, orders have been checked, and any failover has been reviewed.

SCENARIO E: WAREHOUSE SYSTEM LOSS

The WMS at the central warehouse fails or cannot be trusted. Stores and the online store may still work.

Signs

- Pick lists and handheld scanners stop working.
- Stock levels online and in stores stop matching what is in the warehouse.

First actions

1. Warehouse Shift Manager moves to paper picking (document 02, section 6).
2. Incident Lead decides whether to limit online orders for items held only in the warehouse.
3. Tell carriers about any change to collection times or manifests.

What still works

- Stores and their own stock; the online store, if it can show limited stock.
- Phones, radios and paper at the warehouse.

Workarounds

- Picking from the latest exports put on the drive, with a second-person check.
- Prioritise store replenishment for the busiest stores, and orders already promised.

Stand down when the WMS is confirmed sound, paper picks have been entered, and stock has been reconciled.

SCENARIO F: BOTH CLOUDS LOST AT ONCE

Both AWS and Azure services are unavailable or cannot be trusted, for example because of a shared network fault, a large internet disruption or a cyber event.

Signs

- The online store, order management, email, Teams and the intranet are all down together.
- Store and warehouse internet links may also be failing.

First actions

1. Start document 02 and set stores to **Restricted**.
2. Open the out-of-band bridge and the SMS cascade.
3. Assume the outage may last hours. Plan for the rest of the trading day and tomorrow's rotas.
4. If there is any sign of a cyber event, follow Scenario A too.

What still works

- Preptorum drives: this pack, price lists, rotas, contact sheets and templates.
- Cash, and offline card if your terminals and provider allow it.
- Store phones and personal mobiles.

Workarounds

- Run stores on cash and offline card, the warehouse on paper, and communications by phone and SMS.

- Agree a fixed update time each hour (example) with Regional Managers.

Stand down when both platforms are confirmed sound, systems have been reopened in steps, and every paper record has been entered and checked.