Preptorum

FIRST-HOUR RUNBOOK: PEAK-SEASON CYBER ATTACK

EXAMPLE PACK: PELLBROOK & MARR
DOCUMENT 02
FICTIONAL · NOT A REAL COMPANY

Tills, online orders and warehouse down · Pellbrook & Marr · Continuity pack document 02

> **FICTIONAL EXAMPLE CONTENT – Pellbrook & Marr is not a real company.** Roles, limits and timings are invented examples. A real retailer replaces every detail with its own approved procedures and its payment provider's instructions.

Use this runbook when tills, the online store, order management or the warehouse management system (WMS) are down or cannot be trusted, especially in peak season, for any reason: a cyber attack, a cloud outage, a network fault or a software fault. If you are unsure whether it applies, start it. Standing down early costs little; starting late costs a lot.

The aim: keep the shops open and safe, stop the attack spreading, and keep customers informed.

1. WHO DECIDES

ROLE	DECIDES	STAND-IN IF ABSENT
Incident Lead (duty Retail Operations Director, head office)	Declares the incident; sets the trading mode for stores (Normal, Restricted, Closed); pauses online orders and click-and-collect	Deputy duty director
Technology On-Call Lead	Diagnosis, containment with the cyber response lead, recovery estimate	Platform on-call engineer
Cyber response lead	What may be switched off, disconnected or restored	Deputy cyber response lead
Store Operations Lead	Instructions to regional managers and stores	Duty regional manager
Regional Managers	Support to stores in their region; store closure decisions with the Incident Lead	Senior store manager in the region
Store Manager (in each store)	Running the store, staff and customer safety, closing the store if it is unsafe	Duty supervisor
Warehouse Shift Manager	Paper picking, dispatch, carrier liaison	Shift team leader
Online and Customer Service Lead	Online order pause, customer messages, contact centre	Customer service duty manager
People Duty Lead	Rotas, shift messages, staff welfare	People team on call
Finance Duty Lead	Cash floats, cash collections, offline card rules, paper refunds	Finance on call
Communications Lead	Press and social media holding lines	Communications duty officer
Data Protection Lead	Data breach assessment and notifications under our own procedures	Legal duty counsel

Rules of authority

- One Incident Lead at a time. Hand over explicitly, out loud and in the log (see document 04).
- Only the Incident Lead changes the trading mode for all stores. A Store Manager can always close their own store if it is unsafe, and tells the Regional Manager straight away.
- Only the cyber response lead decides what is switched off, disconnected or restored.
- If the Incident Lead cannot be reached within 5 minutes (example), the most senior head-office operations role on duty takes the role until relieved.

2. HEAD OFFICE: THE FIRST HOUR, MINUTE BY MINUTE

0–5 MINUTES: CONFIRM AND DECLARE

- ☐ **Anyone:** report the problem to the Technology On-Call Lead by phone. Do not wait for email or Teams.
- ☐ **Incident Lead:** declare a peak-season cyber incident and note the time.
- ☐ **Incident Lead:** set stores to **Restricted**: stay open, cash and offline card only, no refunds or exchanges for now.
- ☐ **Incident Lead:** open the out-of-band bridge (document 04, section 3) and start the call tree.

- [ ] **Store Operations Lead:** send the first SMS to all store managers and regional managers (template in document 04, section 4).
- [ ] **Incident Lead:** start the paper incident log, or the log template on this drive.

5–15 MINUTES: CONTAIN AND HOLD

- [ ] **Cyber response lead and Technology On-Call Lead:** start containment. Nobody switches off, wipes or reconnects systems without their say.
- [ ] **Online and Customer Service Lead: pause online orders and click-and-collect** (section 5). Put up the holding message.
- [ ] **Warehouse Shift Manager:** move to **paper picking** (section 6).
- [ ] **Communications Lead:** prepare the first customer and press holding lines (section 8). Do not issue anything that guesses at the cause.
- [ ] **Data Protection Lead:** start the data breach assessment in our own procedures.

15–30 MINUTES: STEADY THE STORES

- [ ] **Regional Managers:** call each store in their region. Check: open or closed, payment method working, queues, staff numbers, anything unsafe.
- [ ] **Finance Duty Lead:** confirm cash float top-ups and cash collection changes with the cash collection company.
- [ ] **People Duty Lead:** send the first shift message (section 7) and confirm cover for the next shifts.
- [ ] **Technology On-Call Lead:** give the Incident Lead a first view: what is affected, what is contained, and an honest recovery estimate with its confidence.

30–60 MINUTES: PLAN THE DAY

- [ ] **Incident Lead:** confirm the trading mode for the rest of the day: stay Restricted, close named stores, or return towards Normal if systems are confirmed clean.
- [ ] **Online and Customer Service Lead:** send the first message to customers with open orders and click-and-collect parcels.
- [ ] **Warehouse Shift Manager:** report paper picking progress and carrier collection times.
- [ ] **Incident Lead:** plan the head-office handover if the incident will run past the shift (document 04).
- [ ] **Incident Lead:** set the next update time and tell everyone on the bridge.

3. STORE MANAGER: THE FIRST HOUR

0–5 MINUTES

- [ ] Keep the doors open unless the store is unsafe. Crowds and queues come first.
- [ ] Stop using any till that is behaving strangely. Do not switch it off or unplug it unless head office tells you to.
- [ ] Put up the **"cash and card offline"** sign from the incident folder.
- [ ] Start the paper store log: time, what happened, what you did.

5–15 MINUTES

- [ ] Brief the team at the front of the store: what is down, how we take payment, who to ask.
- [ ] Open the **price list on the drive** for the store, and the current promotions list.
- [ ] Give each payment point a paper sales book, a calculator and a cash bag.
- [ ] Tell click-and-collect customers what is happening, using the holding line.

15–30 MINUTES

- [ ] Call your Regional Manager if they have not called you: open, payment working, queues, staff, anything unsafe.
- [ ] Check the cash float. Ask Finance through your Regional Manager if you need more.
- [ ] Move staff to the busiest payment points and to queue management.

30–60 MINUTES

- [ ] Do a cash check and record it in the store log.
- [ ] Check the next shifts are covered; read out the shift message from head office.
- [ ] Keep every paper sales record together for entering later.

4. TAKING PAYMENT WITHOUT TILLS

- **Cash-only fallback:** take cash at payment points with a paper sales book. Write each sale: time, items, price, amount taken and change given. Two people count cash at every handover between staff.
- **Offline card fallback:** use card terminals in offline mode **only if your terminals and payment provider support it**, and only within the limits your provider has agreed (example: a per-transaction limit). Follow the offline payment instructions on the drive. Keep every terminal receipt.
- **Prices:** use the price and promotion lists on the drive. Do not invent discounts; if a price is not on the list, ask the duty supervisor.
- **Receipts:** give a handwritten receipt from the sales book if the customer asks.
- **Refunds and exchanges:** paused in Restricted mode. Take the customer's details on the paper log and tell them we will contact them.
- **Gift cards and loyalty points:** not accepted until systems return. Say so on the sign.
- **Cash handling:** keep cash in bags at payment points; move it to the safe at set times (example: every hour) with two staff present.

5. PAUSING ONLINE ORDERS AND CLICK-AND-COLLECT

- The Online and Customer Service Lead pauses new online orders and click-and-collect bookings, by switching the online store to its holding page if it still works, or by asking the hosting team to do so.
- Customers with open orders get a short, factual message using the approved template.
- Click-and-collect parcels already in stores can be handed over against the customer's name and order number on the printed or drive-held collection list, checked by a second person. If there is no list, take the customer's details and tell them we will contact them.
- No online refunds are processed until systems are confirmed clean.

6. WAREHOUSE PICKING ON PAPER

- The Warehouse Shift Manager uses the most recent order and stock lists available outside the WMS: printed reports, or exports put on the drive by our own systems or staff (example: at the start of each shift).
- Pickers use paper pick sheets, one order per sheet, and tick each line.
- A second person checks every picked order against its sheet before it is packed.
- Prioritise store replenishment for the busiest stores and orders already promised to customers, as agreed with the Incident Lead.
- Hand-write carrier manifests where labels cannot be printed, and agree this with each carrier.
- Keep every sheet. Stock is reconciled when the WMS is back.

7. STAFF ROTAS AND SHIFT MESSAGES WITHOUT THE INTRANET

- The People Duty Lead sends shift messages by SMS cascade and through Regional Managers, using the templates on the drive.
- Store Managers use the rota printed or saved to the drive for the week (example: refreshed each Friday by the People team).
- Staff call the store phone, not the intranet, to confirm shifts.
- Offer extra shifts first to staff already trained in paper sales and cash handling.
- Watch for tired staff in long days; plan breaks from the first hour.

8. CUSTOMER AND PRESS HOLDING LINES

- Short and factual: what is affected, what we are doing, what customers should do, and when we will update next.
- Do not guess at the cause, the recovery time, or whether data was taken.
- Only the Communications Lead speaks to the press. Store staff pass press enquiries to the Store Manager, who passes them on.

Example customer line (in store): "Our tills are not working normally today. We are open and taking cash, and card payments where our terminals allow. Refunds and exchanges will be available again soon."

Example online line: "We have paused new orders while we fix a technical problem. If you have an order with us, we will contact you by [time]. Our stores are open."

Example press line: "We are dealing with a technical problem affecting some of our systems. Our stores are open and our teams are working to restore normal service. We will share more when we can."

9. STANDING DOWN

The Incident Lead stands the incident down only when:

- the cyber response lead confirms systems are clean and restored from trusted backups;
- tills, the online store and the WMS are confirmed sound by the Technology On-Call Lead;
- paper sales, refunds owed, click-and-collect handovers and paper pick sheets have been entered and checked by a second person;
- online orders and click-and-collect have been reopened in steps;
- customers, staff and, where needed, regulators have had a closing message under our own procedures.

Then hold a short review within two working days (example) and update this runbook.