Exercise report

Operation: Home Front

Data compromise through remote working vulnerabilities

Sector: Transport and logistics
Scenario type: Home and remote working
Date: 3 May 2026
Duration: 20m 25s
Overall rating: Strong decision-making
Decisions made: 6

Facilitator debrief summary

Wins

• Public trust held at 60%
• Threat containment improved by 45 points
• Confident calls — 67% rated 4 or higher

Confidence

Confidence: averaged 3.8/5 across 6 of 6 calls and built from 2/5 to 5/5.

Speed

Speed: 6 decisions in 20m 25s — average 177s per call (fastest 19s, slowest 251s).

Next actions

Next: in your debrief, walk through "Early conservative choices created room to manoeuvre later.; Stakeholder communications stayed ahead of the news cycle." and agree one named owner and a date for each.

Participants

Who was in the room.

Name	Role / function

This report captures the decisions, discussion points, and outcomes from your tabletop exercise. It is designed as a working document — use the space provided to add your own reflections, action items, and follow-up notes. Share it with your team, your senior leadership, and anyone responsible for your organisation's incident response capability.

Scenario briefing

Your organisation supports flexible and remote working. An employee working from home has their home broadband router compromised by an attacker who uses it to intercept network traffic. The employee has been accessing corporate systems, email, and sensitive documents over this compromised connection for several days before the issue is detected.

Before reading on:

What was your team's initial reaction to this scenario? Did it feel realistic? Were there any immediate gaps in your current preparedness?

Outcome

Textbook response

Sustained, measured decision-making kept the situation contained and stakeholder trust intact. (Path taken: 5 cautious, 1 balanced calls.)

Team reflection:

How well does this outcome reflect what would happen in your organisation? What would you do differently if this happened for real?

Impact metrics — start vs end

How each metric moved from the start of the exercise to the final score after every decision.

Public trust	60% →	60%	(0)	
Operational capacity	80% →	55%	(-25)	
Threat containment	40% →	85%	(+45)	

Public trust took a moderate hit (60%). While the situation was managed, there are likely questions about transparency, speed of communication, or the quality of the response. Rebuilding confidence will require proactive engagement.

Operations were noticeably affected (55%). Some services were degraded or interrupted. Staff may be stretched, workarounds are in place, and full recovery will take time and focused effort.

The threat was well contained (85%). Your decisions effectively limited the scope and impact of the incident. The attack surface was reduced and further escalation was prevented.

Metrics reflection:

Which metric concerns you most? What specific actions could your organisation take to improve it?

Why this outcome

Cumulative gains on threat containment (+45) and a final threat containment of 85% put you on this outcome path.

Public trust - 60% -> 60% (+0)

Final band: Strained. Cumulative loss -5, gain +5.

Top drivers:

#4 Respond to enquiries as they come in (-5)
#6 Risk-based remote working tiers (+5)

Operational capacity - 80% -> 55% (-25)

Final band: Strained. Cumulative loss -25, gain +0.

Top drivers:

#2 Targeted investigation of the 14 at-risk staff (-10)
#1 Enforce VPN and reset credentials (-5)
#3 File on time with minimum detail, delay individual notification (-5)

Threat containment - 40% -> 85% (+45)

Final band: Healthy. Cumulative loss -0, gain +45.

Top drivers:

#1 Enforce VPN and reset credentials (+10)
#2 Targeted investigation of the 14 at-risk staff (+10)
#5 Phased rollout starting with high-risk roles (+10)

What you did well

The objective of this exercise is to make decisions, not to save the day. These are the wins your decisions earned — and what would have happened without them.

1. Public trust held at 60%

Under pressure, your decisions kept public trust stable rather than letting it slide.

If you hadn't: Without those calls, communications would likely have lagged behind events — leaving stakeholders, customers and the press to fill the silence with speculation.

2. Threat containment improved by 45 points

You moved threat containment from 40% to 85% through the decisions you committed to.

If you hadn't: Without those calls, the threat would have continued to spread — more systems compromised, more data at risk, longer dwell time for the attacker.

3. Confident calls — 67% rated 4 or higher

Across 6 decisions you rated yourselves, the team backed its judgement. That's a sign the framework matched the situation, not luck.

If you hadn't: Low-confidence decisions tend to get re-litigated mid-incident, costing time and pulling leaders away from the next problem.

Avoided outcomes

Worst-case consequences your decisions prevented — based on the alternative paths not taken and where the headline metrics finished.

1. Sidestepped a medium-risk path at "Decision point: Immediate containment" [LOW] decision #1

Worst case prevented:

The alternative on the table — “Suspend remote access and investigate fully” — would likely have immediately suspend the employee's remote access. require them to work from the office while the investigation is completed. audit all data accessed during the affected period, locking the team into a medium-risk trajectory.

Instead you:

You chose “Enforce VPN and reset credentials” (low risk), keeping options open and avoiding that escalation.

2. Sidestepped a medium-risk path at "Decision point: Regulatory notification" [LOW] decision #3

Worst case prevented:

The alternative on the table — “File immediately and notify all affected individuals” — would likely have submit the ico breach report now with the information available. notify all 230 staff individually. contact affected passengers proactively. accept you may need to file supplementary reports as investigation continues, locking the team into a medium-risk trajectory.

Instead you:

You chose “File on time with minimum detail, delay individual notification” (low risk), keeping options open and avoiding that escalation.

3. Sidestepped a medium-risk path at "Decision point: Multi-stakeholder communications" [LOW] decision #4

Worst case prevented:

The alternative on the table — “Coordinated proactive communications to all audiences” — would likely have issue an all-staff communication explaining what happened, what data was affected, and what you are doing. brief affected passengers individually. prepare a holding statement for media. meet the union representative, locking the team into a medium-risk trajectory.

Instead you:

You chose “Respond to enquiries as they come in” (low risk), keeping options open and avoiding that escalation.

4. Avoided uncontrolled threat spread [HIGH]

Worst case prevented:

If containment had collapsed below 20%, the attacker would have continued lateral movement — more systems compromised, longer dwell time, and a far larger forensic and recovery bill.

Instead you:

You held containment at 85%, cutting off enough of the attack surface to limit the blast radius.

5. Avoided a public trust collapse [MEDIUM]

Worst case prevented:

Below 20% trust, customers, regulators and the press start setting the narrative for you — refunds, churn, regulator scrutiny, and brand damage that takes years to rebuild.

Instead you:

You finished on 60% trust (started at 60%), keeping the room for the organisation to lead its own communications.

6. Avoided operational standstill [MEDIUM]

Worst case prevented:

Below 20% operational capacity, services degrade to the point staff are firefighting unguided and recovery starts from zero — every hour compounds the lost revenue and goodwill.

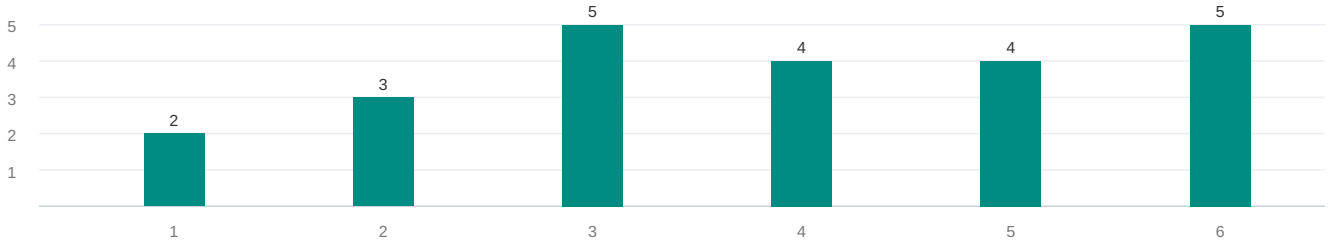
Instead you:

You held operational capacity at 55%, keeping enough of the business running to support a structured response.

Confidence evolution

How the team's self-rated confidence (1–5) moved across each decision. A rising line suggests the team grew into the situation; a falling line is a debrief signal.

START	END	AVERAGE	PEAK	TROUGH	DELTA	TREND
2/5	5/5	3.8/5	5/5	2/5	+3	rising



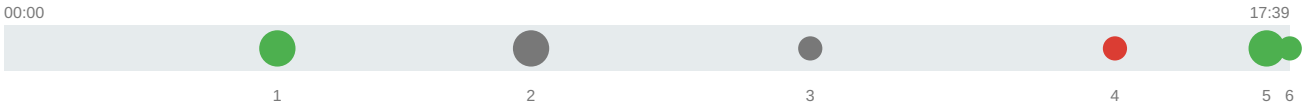
Across 6 of 6 decisions the team rated themselves, confidence started at Low (2/5), ended at Very high (5/5), and averaged 3.8/5 (peak 5/5, trough 2/5). Confidence built across the exercise — a sign the team grew into the situation as the picture clarified.

Decision timeline & rating

When each call was made, how long it took, and how it shifted the running rating. Each decision contributes a score: cautious (+2), balanced (+1), aggressive (-1); the running ratio against the maximum determines the band.

Mix: 5 cautious (+10) | 1 balanced (+1) | 0 aggressive (-0)

TOTAL	AVERAGE	FASTEST	SLOWEST
17:39	02:57	#6 · 00:19	#4 · 04:11



#	Elapsed	Took	Decision	Risk	Impact	Conf.	Δ	Run	Rate
1	03:45	03:45	Enforce VPN and reset credentials	low	+5	2/5	+2	2/2	Excellent
2	07:14	03:29	Targeted investigation of the 14 at-risk staff	medium	0	3/5	+1	3/4	Excellent
3	11:04	03:50	File on time with minimum detail, delay	low	0	5/5	+2	5/6	Excellent
4	15:15	04:11	Respond to enquiries as they come in	low	-5	4/5	+2	7/8	Excellent
5	17:20	02:05	Phased rollout starting with high-risk roles	low	+5	4/5	+2	9/10	Excellent
6	17:39	00:19	Risk-based remote working tiers	low	+15	5/5	+2	11/12	Excellent

Key calls — biggest swings

#2 at 07:14 — "Targeted investigation of the 14 at-risk staff" (0 net, 20 total swing)

#1 at 03:45 — "Enforce VPN and reset credentials" (+5 net, 15 total swing)

#5 at 17:20 — "Phased rollout starting with high-risk roles" (+5 net, 15 total swing)

6 decisions over 17:39, averaging 02:57 per call. 3 of 6 decisions had a net positive impact on the headline metrics. The quickest call (#6, 00:19) was "Risk-based remote working tiers"; the longest deliberation (#4, 04:11) was "Respond to enquiries as they come in". The biggest swings came from #2, #1, #5 — these are the calls that moved the headline metrics most.

Decisions made

Decision 1: Decision point: Immediate containment

decision stage: Assessment | Risk level: low

Chosen: Enforce VPN and reset credentials

Require the employee to use a VPN for all connections. Reset their credentials and session tokens. Continue remote working with enhanced monitoring.

Impact: Trust: +0 | Operations: -5 | Containment: +10 | Confidence: Low

Group vote (20 votes cast):

- Suspend remote access and investigate fully: 6 votes (30%)
- Advise the employee and continue monitoring: 7 votes (35%)
- **> Enforce VPN and reset credentials: 7 votes (35%)**

Scoring rationale: This was the lowest-risk option. It prioritised caution and thoroughness, with a positive or neutral impact on trust and containment.

Options not taken:

- Suspend remote access and investigate fully (medium risk)
  Immediately suspend the employee's remote access. Require them to work from the office while the investigation is completed. Audit all data accessed during the affected period.
- Advise the employee and continue monitoring (low risk)
  Advise the employee to reset their router and change passwords. Continue monitoring for suspicious activity but do not disrupt their work pattern.

Reflect on decision 1:

Why did the group choose this option? What alternatives were discussed? What would you change with hindsight?

Decision 2: Decision point: Escalation and wider risk

decision stage: Powers and policy | Risk level: medium

Chosen: Targeted investigation of the 14 at-risk staff

Investigate the 14 staff with the same router model. Brief the CISO and CTO but hold off on board notification until the scope is confirmed.

Impact: Trust: +0 | Operations: -10 | Containment: +10 | Confidence: Moderate

Group vote (20 votes cast):

- **> Targeted investigation of the 14 at-risk staff: 11 votes (55%)**
- Full estate audit and proactive board briefing: 0 votes (0%)
- Focus on the confirmed compromise only: 9 votes (45%)

Scoring rationale: This was a moderate-risk option. It balanced speed and caution, with mixed impacts across the outcome metrics.

Options not taken:

- Full estate audit and proactive board briefing (medium risk)
  Audit all remote connections for the past 30 days. Brief the board immediately. Treat all 14 staff with the same router model as potentially compromised and suspend their remote access.

- Focus on the confirmed compromise only (low risk)
  Continue investigating the single confirmed compromise. Address the other 14 staff through routine security guidance. Do not escalate to the board at this stage.

Reflect on decision 2:

Why did the group choose this option? What alternatives were discussed? What would you change with hindsight?

Decision 3: Decision point: Regulatory notification

decision stage: Powers and policy | Risk level: low

Chosen: File on time with minimum detail, delay individual notification

Submit a minimal initial report to the ICO within the deadline. Delay individual notification until the investigation is complete so you can provide accurate details.

Impact: Trust: +0 | Operations: -5 | Containment: +5 | Confidence: Very high

Group vote (0 votes cast):

- File immediately and notify all affected individuals: 0 votes (0%)
- Seek a deadline extension before filing: 0 votes (0%)
- **> File on time with minimum detail, delay individual notification: 0 votes (0%)**

Scoring rationale: This was the lowest-risk option. It prioritised caution and thoroughness, with a positive or neutral impact on trust and containment.

Options not taken:

- File immediately and notify all affected individuals (medium risk)
  Submit the ICO breach report now with the information available. Notify all 230 staff individually. Contact affected passengers proactively. Accept you may need to file supplementary reports as investigation continues.

- Seek a deadline extension before filing (low risk)
  Contact the ICO to request additional time. Explain the investigation is ongoing. Do not notify individuals until the full picture is clear.

Reflect on decision 3:

Why did the group choose this option? What alternatives were discussed? What would you change with hindsight?

Decision 4: Decision point: Multi-stakeholder communications

decision stage: Options | Risk level: low

Chosen: Respond to enquiries as they come in

Respond to each audience as they contact you. Provide factual information on a case-by-case basis. Do not issue a proactive all-staff communication.

Impact: Trust: -5 | Operations: +0 | Containment: +0 | Confidence: High

Group vote (20 votes cast):

- Coordinated proactive communications to all audiences: 2 votes (10%)
- Restrict information to those directly affected: 5 votes (25%)
- **> Respond to enquiries as they come in: 13 votes (65%)**

Scoring rationale: This was the lowest-risk option. It prioritised caution and thoroughness, with a positive or neutral impact on trust and containment.

Options not taken:

- Coordinated proactive communications to all audiences (medium risk)
  Issue an all-staff communication explaining what happened, what data was affected, and what you are doing. Brief affected passengers individually. Prepare a holding statement for media. Meet the union representative.

- Restrict information to those directly affected (medium risk)
  Notify only the 230 staff whose personal data was exposed. Tell passengers only if they ask. Decline media comment. Defer the union meeting.

Reflect on decision 4:

Why did the group choose this option? What alternatives were discussed? What would you change with hindsight?

Decision 5: Decision point: Investing in remote working security

decision stage: Options | Risk level: low

Chosen: Phased rollout starting with high-risk roles

Approve a phased VPN rollout starting with roles that handle sensitive data. Provide enhanced guidance for other remote workers. Review after six months.

Impact: Trust: +0 | Operations: -5 | Containment: +10 | Confidence: High

Group vote (20 votes cast):

- **> Phased rollout starting with high-risk roles: 15 votes (75%)**
- Full investment in mandatory VPN and device management: 3 votes (15%)
- Defer investment and rely on updated guidance: 2 votes (10%)

Scoring rationale: This was the lowest-risk option. It prioritised caution and thoroughness, with a positive or neutral impact on trust and containment.

Options not taken:

- Full investment in mandatory VPN and device management (medium risk)
  Approve the £180,000 VPN infrastructure. Mandate VPN for all remote connections. Implement mobile device management for all corporate devices used remotely. Frame it as investment in flexible working, not restriction.

- Defer investment and rely on updated guidance (low risk)
  Defer the major investment. Issue comprehensive remote working security guidance. Rely on staff awareness and existing tools.

Reflect on decision 5:

Why did the group choose this option? What alternatives were discussed? What would you change with hindsight?

Decision 6: Decision point: Long-term remote working strategy

decision stage: Action and review | Risk level: low

Chosen: Risk-based remote working tiers

Create tiered remote working categories based on role sensitivity. Higher-risk roles get corporate devices and mandatory VPN. Lower-risk roles get enhanced guidance and monitoring.

Impact: Trust: +5 | Operations: +0 | Containment: +10 | Confidence: Very high

Group vote (0 votes cast):

> Risk-based remote working tiers: 0 votes (0%)
- Maintain current approach with better awareness: 0 votes (0%)
- Zero-trust remote access architecture: 0 votes (0%)

Scoring rationale: This was the lowest-risk option. It prioritised caution and thoroughness, with a positive or neutral impact on trust and containment.

Options not taken:

- Zero-trust remote access architecture (medium risk)
  Implement a zero-trust model where every connection is verified regardless of location. Invest in always-on VPN, device compliance checks, and conditional access. Frame it as a modern, flexible infrastructure.

- Maintain current approach with better awareness (low risk)
  Keep the current flexible approach but improve security awareness training. Rely on staff to follow best practice. Accept residual risk.

Reflect on decision 6:

Why did the group choose this option? What alternatives were discussed? What would you change with hindsight?

Decision-quality scoreboard

Each decision is rated on three axes derived from the Law Enforcement Decision Techniques: rigour (did the team consider risk and alternatives), outcome (did the call move the metrics in a defensible direction) and confidence calibration (was stated confidence well matched to outcome). Heuristic — provoke debrief, not a performance review.

Aggregate score: 66/100 — SOUND

Defensible call. Process and outcome both reasonable.

exemplary	strong	sound	mixed	develop
0	1	5	0	0

#	Decision	Rigour	Outcome	Calib.	Total	Rating
1	Enforce VPN and reset credentials	75	55	70	**66**	**sound**
2	Targeted investigation of the 14 at-risk staff	75	50	100	**70**	**strong**
3	File on time with minimum detail, delay individual notification	75	50	50	**60**	**sound**
4	Respond to enquiries as they come in	75	45	70	**62**	**sound**
5	Phased rollout starting with high-risk roles	75	55	80	**68**	**sound**
6	Risk-based remote working tiers	75	65	65	**69**	**sound**

Highest-scoring calls

#2 Targeted investigation of the 14 at-risk staff — 70/100
#6 Risk-based remote working tiers — 69/100
#5 Phased rollout starting with high-risk roles — 68/100

Lowest-scoring calls (debrief focus)

#3 File on time with minimum detail, delay individual notification — 60/100
#4 Respond to enquiries as they come in — 62/100
#1 Enforce VPN and reset credentials — 66/100

Score rationale per decision

Decision 1 — Enforce VPN and reset credentials (66/100, sound)

- Considered three or more options before committing.
- Decision was put to the room.

Decision 2 — Targeted investigation of the 14 at-risk staff (70/100, strong)

- Considered three or more options before committing.
- Decision was put to the room.
- Confidence was well calibrated to the outcome.

Decision 3 — File on time with minimum detail, delay individual notification (60/100, sound)

- Considered three or more options before committing.
- Decision was put to the room.

Decision 4 — Respond to enquiries as they come in (62/100, sound)

- Considered three or more options before committing.
- Decision was put to the room.

Decision 5 — Phased rollout starting with high-risk roles (68/100, sound)

- Considered three or more options before committing.
- Decision was put to the room.

Decision 6 — Risk-based remote working tiers (69/100, sound)

- Considered three or more options before committing.
- Decision was put to the room.
- Decision pushed the metrics meaningfully forward.

Total crisis cost

Scale: Mid-market. Eight categories of exposure modelled from final metrics, sector, scenario type and time on incident. Heuristic estimates intended to provoke debrief discussion - not actuarial figures.

Total exposure: £1.04m (£1,041,577)

mostly long-tail damage — 63% of the cash-vs-trust split arrives in the months after the incident, not on the day. The single biggest line is regulatory fines & legal fees.

≈ 1.4% of annual revenue — a material but recoverable hit.

Immediate cash exposure: £380k (response + downtime + technical + people)

Long-tail exposure: £661k (churn + regulatory + reputation + insurance)

Decisions logged: 6 | Direct response cost: £57k

Where the money went

#1 Regulatory fines & legal fees

£316k (30.3% of total)

Recurrence: One-off

Sector exposure (1.1×) and a 28% trigger drive likely ICO/sector-regulator action plus external counsel costs. The trigger is squared (^1.6) so moderate breaches produce moderate fines, reflecting ICO's actual enforcement curve. Capped at the greater of ICO's £17.5m statutory maximum or 4% of annual revenue (GDPR Art. 83(5)). Not a guaranteed fine — a planning estimate.

Formula: min(max fine × trigger^1.6 × 0.55 × max(sector reg, scenario reg), max(£17.5m, 4% × ARR))

- Max regulatory ceiling: £4,000,000 (Typical exposure for Mid-market band)
- Trigger strength: 28% (max(containment gap 15%, trust damage × 0.7))
- Sector regulatory weight: 1.10×
- Scenario-type weight: 1.00× (Cyber/data incidents amplify regulator interest.)
- Effective regulatory weight: 1.10× (max(sector, scenario) — additive, not multiplicative, to stop double-counting.)
- Statutory cap: £17,500,000 (max(£17.5m ICO max, 4% × ARR) per GDPR Art. 83(5))
- Containment factor (live): 28% (Used by the live ticker — final containment 85%)

Debrief prompts:

- Were notification clocks acknowledged early, or only when prompted?
- Who would have signed off the regulator-facing narrative?

#2 People & welfare (overtime, EAP, turnover)

£171k (16.4% of total)

Recurrence: One-off

~81 staff × 13h overtime, plus employee assistance and projected turnover replacement costs.

Formula: overtime + EAP uplift + turnover risk

- Affected staff: 81 (headcount 500 × (5% + ops damage × 25%))
- Overtime hours: 13 h (time on incident × 1.5 + decisions × 2 (min 8h))
- Loaded hourly rate: £65/h (UK blended rate including on-cost)
- Overtime cost: £65,867
- EAP / counselling: £25,000 (Headcount × £50 × scenario welfare weight)
- Turnover risk: £80,000 (Headcount × trust damage × £400 × welfare weight)
- Scenario welfare weight: 1.00×

Debrief prompts:

- Did anyone check on the responders' welfare during the exercise?
- Who was running on adrenaline by the end — and what's the plan for them next time?

#3 Reputation & PR recovery

£156k (15.0% of total)

Recurrence: One-off

External comms agency, media monitoring, and paid recovery campaigns to restore brand trust over 6–12 months.

Formula: (0.2% of ARR) × (0.4 + trust damage × 1.6) × scenario rep weight

- Baseline budget: £150,000 (0.2% of annual revenue)
- Trust damage: 40%
- Scenario reputation weight: 1.00×

Debrief prompts:

- Which moment in the exercise did the most reputational damage?
- Was there a missed opportunity to take control of the public story?

#4 Customer churn & lost future revenue

£150k (14.4% of total)

Recurrence: Annualised

Trust drop of 40% drives roughly 0.20% of annual revenue lost over the next 12 months in your sector.

Formula: ARR × (trust damage × 0.5% × sector churn weight)

- Trust damage: 40% (100% − final public trust (60%))
- Sector churn weight: 1.00× (Consumer-facing sectors churn faster than B2B/regulated.)
- Effective churn: 0.20% of ARR
- Annual revenue: £75,000,000

Debrief prompts:

- What single action would have halved the trust drop?
- Who was responsible for protecting customer perception during the incident?

#5 Technical recovery, forensics & rebuild

£122k (11.7% of total)

Recurrence: One-off

Incident response retainer, forensic investigation, and system restoration — sized by containment gap (15%) and incident type.

Formula: (top of per-decision range × 2) × (0.4 + containment gap × 1.1) × scenario tech weight

- Technical baseline: £240,000 (2 × top of per-decision range (£120k) — covers IR retainer + forensics + rebuild for the band.)
- Containment factor (live): 28% (Live ticker uses 1 − 0.85 × (containment ÷ 100))
- Containment gap (final): 15% (100% − final threat containment (85%))
- Scenario technical weight: 0.90×

Debrief prompts:

- Which technical debt got exposed by this incident?
- What would the team rebuild differently if budget were no object?

#6 Direct response (decisions)

£57k (5.5% of total)

Recurrence: One-off

Sum of the 6 decisions the team committed to during the exercise.

Formula: Σ(cost of each committed decision)

- Decisions committed: 6
- Sum of decision costs: £57,000 (Each option's £ comes from its authored cost or risk × impact × scale multiplier.)
- Scale band: Mid-market (Per-decision range £5.0k–£120k)

Debrief prompts:

- Which committed decision do you think was the best value for money — and which the worst?
- Were any of these spends avoidable with earlier action?

#7 Insurance premium uplift

£40k (3.8% of total)

Recurrence: Annualised

Estimated 33% increase on cyber/crisis cover at next renewal (baseline £120k/yr).

Formula: baseline premium × (15% + max(containment gap, trust damage) × 45%)

- Baseline cyber premium: £120,000/yr
- Uplift: 33%
- Worse of containment gap / trust damage: 40%

Debrief prompts:

- Do you actually know what your cyber policy excludes?
- Would this incident trigger a premium reset at your next renewal?

#8 Operational downtime / lost revenue

£30k (2.9% of total)

Recurrence: One-off

Approx 0.2 days of degraded operations at £300k/day, scaled by your final operational capacity (55%).

Formula: daily revenue × ops damage × downtime days

- Daily revenue: £300,000/day (£75.00m ARR ÷ 250 working days)
- Ops damage: 45% (100% − final operational capacity (55%))
- Downtime days: 0.22 days (max(time on incident ÷ 24h, ops damage × 0.5))
- Time on incident: 20.4 min (0.34 h)

Debrief prompts:

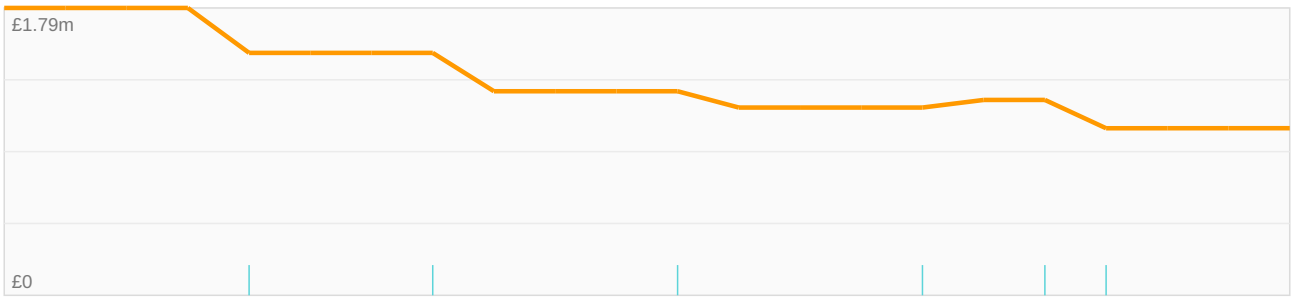
- What would have brought operations back online faster?
- Did anyone own the call to degrade or restore service, or did it drift?

Per-decision response cost

01 Enforce VPN and reset credentials (low)	£13k
02 Targeted investigation of the 14 at-risk staff (medium)	£14k
03 File on time with minimum detail, delay individual notification (low)	£9.0k
04 Respond to enquiries as they come in (low)	£2.0k
05 Phased rollout starting with high-risk roles (low)	£13k
06 Risk-based remote working tiers (low)	£6.0k
Subtotal - direct response	**£57k**

Cost accrual timeline

Minute-by-minute projection of cumulative exposure as the incident progressed, replaying each decision at the time it was actually taken. Use it to spot when the curve flattened (containment achieved) versus when cost was still climbing.



Time	Cumulative cost	Containment
0 min	£1.79m	40%
2 min	£1.79m	40%
5 min	£1.51m	50%
7 min	£1.51m	50%
9 min	£1.27m	60%
12 min	£1.17m	65%
14 min	£1.17m	65%
16 min	£1.22m	65%
19 min	£1.04m	85%
21 min	£1.04m	85%

Decision markers on the timeline

4 min	#1	Enforce VPN and reset credentials	containment +10
7 min	#2	Targeted investigation of the 14 at-risk staff	containment +10
11 min	#3	File on time with minimum detail, delay individual notification	containment +5
15 min	#4	Respond to enquiries as they come in	containment 0
17 min	#5	Phased rollout starting with high-risk roles	containment +10
18 min	#6	Risk-based remote working tiers	containment +10

Final modelled exposure at 21 min: £1,041,577 (started at £1,791,064, ending containment 85%).

Industry benchmarks — your run vs your peers

Compares your final state against Transport and logistics teams running the same scenario. Sample size: undefined prior runs. Averages are only published once three or more peers have completed the scenario, to protect individual teams' results.

Peer averages aren't published yet for this scenario in Transport and logistics — only undefined prior runs have been recorded. The benchmark unlocks at three runs.

Lessons learned

1. Early conservative choices created room to manoeuvre later.
2. Stakeholder communications stayed ahead of the news cycle.
3. Lessons-learned process can move straight to formal capture.

Action planning:

Based on these lessons, what three things will your team commit to doing within the next 30 days?

Supporting your staff

Major incidents take a personal toll. Even staff who weren't directly affected may feel exposed, blamed, or burnt out. Building staff support into the response — not just the debrief — protects wellbeing and makes the team more resilient for the next event.

During the incident

- Make rest and handover mandatory — rotate responders so no one works more than a single shift without a break.

- Feed people. Order food in, keep water and caffeine available, and protect time for meals away from screens.
- Name a single point of contact for staff questions so the response team isn't interrupted constantly.
- Be explicit that nobody will be blamed for the initial incident (e.g. clicking a phishing link). Blame slows reporting on the next event.
- Communicate clearly and often, even when there's nothing new — silence breeds rumour and anxiety.

In the first 72 hours after

- Hold a short, structured 'hot debrief' focused on what happened and what people need now — not on judgement.
- Offer time off in lieu for those who worked extended hours, and protect it (don't pull people back into BAU immediately).
- Signpost your Employee Assistance Programme (EAP), occupational health, and any internal mental-health first-aiders.
- Watch for warning signs: sleep disruption, withdrawal, irritability, or staff repeatedly replaying the incident.
- Thank people specifically and publicly. Generic 'thanks team' messages land flat after a hard week.

Longer term

- Run a 'cold debrief' 2–4 weeks later when emotions have settled and lessons can be captured calmly.
- Review whether on-call rotas, response retainers, or staffing levels need to change so the same people aren't always carrying the load.
- Update the staff member who triggered the incident (if any) on what changed as a result — closes the loop and reinforces no-blame culture.
- Track whether anyone leaves the team in the 6 months after the incident — burnout often surfaces late.
- Build staff support into your incident response plan as a named workstream, with an owner, not as an afterthought.

Resources

HSE — Managing stress at work
https://www.hse.gov.uk/stress/

Mind — Mental health at work
https://www.mind.org.uk/workplace/

NCSC — Cyber security and the human factor
https://www.ncsc.gov.uk/collection/you-shape-security

Further reading

The following resources provide additional guidance relevant to this scenario:

NCSC — Home working: securing your devices
https://www.ncsc.gov.uk/collection/device-security-guidance/bring-your-own-device

ICO — Data protection and home working
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/

Ethical principles - reflection

Use these questions to reflect on whether your decisions upheld ethical standards:

- Is what I am considering consistent with these ethical principles?
- What would my colleagues, customers and stakeholders expect of me in this situation?
- What does my organisation expect of me in this situation?
- Is this action likely to reflect positively on the organisation? Will it affect stakeholder trust?
- Could I explain my action or decision to the board, regulators or affected stakeholders?

Facilitator debrief questions

These questions can be used by facilitators or supervisors during the post-exercise review:

- Did you recognise and acknowledge instances of initiative or good decisions?
- Did you recognise, question and challenge instances of poor decision making?
- Can you relate the decision making to the organisation's ethical principles?
- Are there any opportunities for organisational learning?

Post-incident review

Use this structured post-incident review (PIR) to turn the exercise into lessons learned. Work through each section in order, capture answers in writing, and assign owners + deadlines to every action.

1. Detection & escalation

How quickly did we know, and how quickly did the right people find out?

? How was the incident first detected — was it from monitoring, a user report, a third party, or external notification?

? How long was it between the first signal and the team being mobilised? Where was the time lost?

? Were the right people notified at the right time? Who was missed, and who was over-notified?

? Did our alerting thresholds and on-call rota work as expected? What needs tuning?

2. Decision-making & command

Who was making decisions, on what information, and was that the right setup?

? Was it always clear who held overall command and who held technical lead? Did that change during the incident?

? What information were decision-makers missing? What did they have to guess?

? Were any decisions deferred or avoided? What blocked them?

? Looking back, which decision had the biggest positive impact on the outcome? Why?

? Which decision would you make differently with hindsight, and what would you need to make that call faster next time?

3. Communications

Internal teams, executives, customers, regulators, media — did each get what they needed, when they needed it?

? Was the internal team kept informed without being overwhelmed? How was situational awareness maintained?

? Were executives and the board briefed at the right cadence and level of detail?

? Were customer and external comms clear, accurate, and timely? What was the lag between deciding to communicate and actually doing it?

? Were regulators or law enforcement engaged at the right point? Were obligations met?

? Did pre-prepared holding statements and comms templates exist? Were they used? What was missing?

4. Technical response & containment

What did we actually do to stop the bleeding, and did it work?

? What containment actions were taken, and in what order? Were any reversed or repeated?

? Were the necessary tools, access, and credentials available to the people who needed them, when they needed them?

? Were any actions blocked by change-control, approvals, or a lack of authority? Should those constraints be revisited for incident scenarios?

? Was evidence preserved appropriately for forensic and regulatory purposes?

5. People, roles & welfare

An incident is run by people under pressure. How did that go?

? Did everyone know their role, or were there overlaps and gaps? Where was role clarity weakest?

? Were shifts, handovers, and rest managed — or did key people work past the point of safe judgement?

? Who in the wider organisation needs welfare follow-up after this exercise or incident?

? Who performed above expectation and should be recognised? Who needs additional training or support?

6. Recovery & business continuity

Even if the threat is contained, the organisation isn't back to normal.

? What is our definition of 'recovered'? Have we agreed it, or is that still ambiguous?

? Which business processes were degraded, and which workarounds need to be retired or kept?

? What is the data integrity status? Are we confident in what we restored?

? What's the longer-term reputational, financial, or regulatory exposure we now need to manage?

7. Root cause & systemic factors

Look past the proximate cause. What conditions made this possible?

? What was the proximate trigger? What was the underlying systemic cause?

? Were there warning signs, near-misses, or audit findings that flagged this risk previously? What happened to them?

? What assumptions about our defences turned out to be wrong?

? Is this a one-off, or a symptom of a wider pattern we should investigate?

8. Actions, owners & deadlines

Lessons identified are not lessons learned until something changes. Capture concrete commitments here.

? Immediate (within 7 days): what must change this week? Owner and deadline for each.

? Short-term (within 30 days): what processes, runbooks, or tooling need updating?

? Medium-term (within 90 days): what training, exercises, or capability investment is needed?

? Strategic (within 12 months): what governance, structural, or supplier changes should be considered?

? How will we track these actions to closure, and who owns the follow-up review?

Cost model — sources & assumptions

Every figure in the cost section is a calibrated heuristic, not an actuarial estimate. The sources below are the published guidance and datasets used to set the formulas, multipliers and caps in the cost model.

Direct response (decisions)

Driving assumptions

- Each option's £ comes from the scenario author's per-choice cost, or from risk × impact × scale-band multiplier when not specified.
- Scale band (SME / mid-market / enterprise) sets the per-decision range — see assumptions panel for the band you ran in.

Published sources

- Cyber Security Breaches Survey 2024 — DSIT / Home Office (2024)
  Per-incident response cost ranges by organisation size — used to anchor the per-decision bands.
  https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024
- Cyber Essentials & 10 Steps to Cyber Security — NCSC
  Catalogue of expected response actions priced into the per-decision options.
  https://www.ncsc.gov.uk/collection/10-steps

Operational downtime / lost revenue

Driving assumptions

- Daily revenue = annual revenue ÷ 250 working days.
- Downtime days = max(time on incident ÷ 24h, ops damage × 0.5) — i.e. there is always at least a half-day floor when operations are degraded.
- Ops damage is 100% − final operational capacity metric.

Published sources

- Cost of a Data Breach Report 2024 — IBM Security / Ponemon Institute (2024)
  Lost-business component (~30% of total breach cost) and average mean time to contain (~292 days) — used to size the downtime curve.
  https://www.ibm.com/reports/data-breach
- Annual Cyber Threat Report — NCSC
  Sector-by-sector outage durations from major UK incidents.
  https://www.ncsc.gov.uk/collection/annual-review-2024

Customer churn & lost future revenue

Driving assumptions

- Worst-case (full trust collapse, consumer-facing sector) caps at ~0.75% of ARR — calibrated against IBM's lost-business component (~0.1–0.5% of ARR for the report's enterprise sample).
- Sector churn weight: consumer-facing sectors (retail, telco, consumer financial services) churn faster than B2B / heavily regulated sectors.
- Trust damage is 100% − final public trust metric.

Published sources

- Cost of a Data Breach Report 2024 — Lost business cost — IBM Security / Ponemon Institute (2024)
  Lost-business cost (~$1.47M of $4.88M average total) used as the upper bound for churn as a share of ARR.
  https://www.ibm.com/reports/data-breach
- Consumer trust and post-breach behaviour — PwC Consumer Intelligence Series
  Per-sector churn intent multipliers after a publicised incident.
  https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/consumer-intelligence-series-trust.html

Regulatory fines & legal fees

Driving assumptions

- Statutory cap = max(£17.5m, 4% of annual revenue), per UK GDPR Article 83(5).
- Trigger is squared (^1.6) so a moderate breach (~40% containment gap) yields a moderate fine, reserving the ceiling for genuinely worst-case outcomes — matches ICO's actual enforcement distribution.
- Sector and scenario-type weights are combined as max(), not multiplied, to avoid double-counting.

• Estimate is for planning conversation, not a forecast — actual ICO action depends on cooperation, remediation, and victim harm.

Published sources

• UK GDPR — Article 83 (Administrative fines) — UK Statute / ICO
£17.5m / 4% ARR statutory cap and the tiering structure for fines.
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/enforcement/penalty-notices/
• ICO enforcement action register — Information Commissioner's Office
Distribution of published fines (most £4–20m, only worst hit £20m+) used to shape the trigger curve.
https://ico.org.uk/action-weve-taken/enforcement/
• Data protection fining guidance — ICO (2024)
Aggravating / mitigating factors that informed the sector-weight multipliers.
https://ico.org.uk/about-the-ico/our-information/policies-and-procedures/data-protection-fining-guidance/

Reputation & PR recovery

Driving assumptions

• Baseline budget = 0.2% of annual revenue (typical comms agency retainer + monitoring).
• Multiplier ranges 0.4–2.0× baseline (≈ 0.08–0.4% of ARR) depending on trust damage.
• Reputational scenario weight (e.g. brand-led incidents) further amplifies the figure.

Published sources

• Edelman Trust Barometer — Edelman
Trust-recovery durations and the spend profile of post-incident reputation campaigns.
https://www.edelman.com/trust/trust-barometer
• WPP / Kantar BrandZ — Brand value recovery — Kantar
Indicative comms / paid-media budgets to rebuild brand equity after a publicised incident.
https://www.kantar.com/campaigns/brandz

Technical recovery, forensics & rebuild

Driving assumptions

• Baseline = 2 × top of the per-decision range for the scale band — covers IR retainer + forensics + system rebuild.
• Containment-gap multiplier ranges 0.4–1.5×, so a poorly contained breach inflates costs but does not run away.
• Scenario technical weight reflects how forensics-heavy the incident type is (e.g. ransomware vs. phishing).

Published sources

• M-Trends Report — Mandiant (Google Cloud)
Median dwell time, forensics scope, and rebuild duration for major incidents — used to size the technical baseline.
https://www.mandiant.com/m-trends
• Global Threat Report — CrowdStrike
Per-incident IR retainer and rebuild costs for enterprise breaches.
https://www.crowdstrike.com/global-threat-report/
• Incident management guidance — NCSC
Standard recovery activities priced into the technical baseline.
https://www.ncsc.gov.uk/collection/incident-management

People & welfare (overtime, EAP, turnover)

Driving assumptions

• Affected staff = headcount × (5% + ops damage × 25%) — a floor of 5 staff is always assumed.
• Loaded hourly rate = £65/h (UK blended rate including on-cost).
• EAP / counselling = headcount × £50 × scenario welfare weight.
• Turnover risk = headcount × trust damage × £400 × welfare weight (proxy for replacement cost of stress-driven attrition).

Published sources

• ASHE — Annual Survey of Hours and Earnings — Office for National Statistics
UK loaded-hourly-rate benchmark used for overtime costing.
https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/earningsandworkinghours/bulletins/annualsurveyofhoursandearnings/2024
• Cost of poor mental health to employers in the UK — Deloitte
Per-head EAP / counselling cost and turnover-replacement cost ranges.

https://www.deloitte.com/uk/en/services/consulting/research/mental-health-and-employers.html

Insurance premium uplift

Driving assumptions

- Uplift = 15% + max(containment gap, trust damage) × 45% — i.e. a notifiable incident raises premiums 15–60% at next renewal.
- Applied to the baseline cyber premium for the scale band (or a per-scenario override).
- Annualised — represents one renewal cycle, not the full multi-year impact.

Published sources

- UK Cyber Insurance Market Report — Association of British Insurers (ABI)
  Post-incident renewal uplift bands (commonly 15–60%) and baseline premium ranges by scale.
  https://www.abi.org.uk/products-and-issues/topics-and-issues/cyber-risk/
- Cyber insurance pricing trends — Marsh McLennan
  Historical pricing trajectory and renewal repricing after notifiable events.
  https://www.marsh.com/en/services/cyber-risk/insights.html