

For the board of directors

Worst Day drill: ransomware with data theft

Where we stand

We ran a full-day ransomware drill on a copy of our own systems. Our security team, IT operations, executives and two outside firms worked it together from the first alert to recovery. We sent 2 of 3 required notices on time, 1 of 2 outside firms responded within contract, and 2 of 3 key systems were back within their recovery target.

The drill shows how our people and partners worked on the day. It does not prove our production systems are secure.

How the day went

Required notices sent on time

2 of 3

Partly on time

Regulator initial notification, data protection notice and insurer notice

Outside firms on time

1 of 2

Partly on time

Security monitoring provider and incident response firm, against their contracts

Key systems back on time

2 of 3

Partly on time

Domain controller, trading platform and file server, against recovery targets

What changed

- Last month's attack test found a route from a VPN account to our domain controller that raised no alert. It was still open on the day, and the attacker used it to get in.
- File server backups could be deleted with ordinary domain credentials. The file server came back late, from an older offline copy.
- The insurer notice went out late because no one in our response plan owns it.

What we need from the board

1

Approve separate backup credentials

Put our backup systems on their own sign-in, apart from the company domain, so an attacker who takes the domain cannot delete our backups.

Owner: Sam Okafor, IT operations lead

2

Confirm an owner for the insurer notice

Name one executive who sends the insurer notice inside the policy's 4-hour window. The response plan is updated to match.

Owner: Priya Anand, general counsel

Decisions taken on the day

05:15	The ransom demand: Refuse. Restore from backup. Tomas Reyna (CEO, with general counsel)
05:25	Restore order: dc01, then the trading platform, then fs01. Ines Marlow (Incident lead)
05:40	Public statement: Publish the holding statement. Jonah Albers (Head of communications)
07:50	DORA initial notification: Send the initial notification now. Priya Anand (General counsel)

Gaps and fix status

Each gap from the drill has an owner and a check that proves the fix. A gap closes only when that check passes. 0 of 5 closed.

Gap	Owner	Next step	Status
A route from a VPN account to the domain controller raises no alert	Rafa Lind	Fix the detection, then retest in Attack Testing	Open, retest after the fix
Large data transfers out of the file server raise no alert	Rafa Lind	New detection, retested in the next attack test	Open, retest after the fix
No one owns the insurer notice in the response plan	Priya Anand	Plan update, checked in the next Worst Day	Open, checked in the next drill
File server backups could be deleted with ordinary domain credentials	Sam Okafor	Separate the backup credentials, checked in the next Black Start	Open, checked in the next recovery test
The incident response firm arrived later than its retainer allows	Ines Marlow	Raise with the firm; timed again in the next drill	Open, checked in the next drill

How to read these results

What the drill shows

- How our teams, executives and outside firms worked together against the clock.
- Which deadlines, contracts and recovery targets held on the day, with the times behind each.
- Where our response plan has gaps, and who owns each fix.

What it cannot show

- That our production systems are secure.
- How a different attack, or a different day, would play out.
- Anything about systems that were left out of the copy.

Appendix

Key events on the day

Times are scenario times. The drill ran from 02:14 to 11:30.

02:14	● Providers	MDR provider: EDR on fs01 flags a credential theft tool. The alert reaches the MDR provider and the escalation timer starts.
02:41	● Providers	MDR provider: Calls Mei Tan, CoinExchange's on-call analyst. Escalation took 27 minutes, inside the 30-minute contract.
02:47	● SOC	Mei Tan: Triage the alert in the SIEM and sees large outbound transfers from fs01.
02:58	● SOC	Rafa Lind: Escalates to the incident lead.
03:05	● Leadership	Ines Marlow: Declares a major incident. The DORA initial notification and insurer notice clocks start, and leadership is paged.
03:12	● Leadership	Ines Marlow: Calls the incident response firm. The retainer timer starts.
03:40	● Attacker	Attacker (operator): Pushes ransomware through group policy from dc01. dc01, fs01, trade-app and trade-db go down, and a Black Start clock starts for each.
03:52	● SOC	Rafa Lind: Isolates the server segment and disables the VPN account j.berger.
04:05	● Exercise control	Exercise control: Inject released: Leak site post
04:05	● Exercise control	Exercise control: Inject released: Ransom note
04:30	● SOC	Mei Tan: Confirms customer and employee records left fs01. The GDPR 72-hour clock starts.
04:40	● Providers	Incident response firm: Responder joins the bridge 88 minutes after the call, outside the retainer's 60 minutes.
05:15	● Leadership	Tomas Reyna: Decided: Refuse. Restore from backup. Backups for the systems that matter look intact, paying does not stop the leak, and counsel advises against it.
05:20	● Exercise control	Exercise control: Inject released: Request for comment
05:25	● Leadership	Ines Marlow: Decided: dc01, then the trading platform, then fs01. Nothing else authenticates without dc01; trading is the business priority after that.
05:30	● IT operations	Sam Okafor: Black Start begins: restoring dc01 from backup.
05:40	● Leadership	Jonah Albers: Decided: Publish the holding statement. Silence reads as hiding it once the post is public.
06:10	● IT operations	Sam Okafor: The online backup set for fs01 was deleted by the attacker. Switching to the offline copy.
06:40	● Leadership	Priya Anand: DORA initial notification sent: met with 25 min to spare.
07:05	● IT operations	Sam Okafor: dc01 is back after 3 h 25 min, inside its 4-hour target.
07:05	● Exercise control	Exercise control: The insurer notice deadline passed with nothing sent. Nobody owned it.
07:50	● Leadership	Priya Anand: Decided: Send the initial notification now. We know enough to notify; waiting only risks the 24 hours.
08:30	● Leadership	Elena Voss: Insurer notice sent: 1 h 25 min late.
08:55	● IT operations	Sam Okafor: The trading platform is back after 5 h 15 min, inside its 6-hour target. Trading can resume.
09:40	● Leadership	Priya Anand: GDPR breach notification sent: met with 66 h 50 min to spare.
11:20	● IT operations	Sam Okafor: fs01 is back from the offline copy after 7 h 40 min, past its 6-hour target. Files changed since the offline copy are lost.
11:30	● Exercise control	Exercise control: Ends the drill. The after-action report and Readiness Record entry are drafted from the timeline.

Framework mapping

Where this drill may count as evidence. No line is final until it is confirmed.

Framework	Requirement	What the drill showed	Status
DORA	Article 19: initial notification of a major ICT-related incident to the competent authority	Sent 06:40 by Priya Anand, 25 min inside the window.	Mapping to be confirmed by DeployOpen's compliance team
DORA	Articles 11 and 12: ICT response and recovery plans, backup and restoration	Recovery of 3 key systems rehearsed; 2 of 3 back within target.	Mapping to be confirmed by DeployOpen's compliance team
GDPR	Article 33: notify the supervisory authority within 72 hours of becoming aware of a personal data breach	Sent 09:40 by Priya Anand, 66 h 50 min inside the window.	Mapping to be confirmed by DeployOpen's compliance team