After-action report

CoinExchange · Worst Day: ransomware with data theft · scenario time 02:14 to 11:30

Summary

CoinExchange's SOC, IT operations, leadership and both providers worked a ransomware attack with data theft on a copy of CoinExchange's environment, from the first alert at 02:14 until exercise control ended the drill at 11:30. They met 2 of 3 notice deadlines, 1 of 2 providers worked within contract, and 2 of 3 systems came back within their recovery target.

A drill result shows what the team did in the drill. It does not prove production is secure.

Outcomes

Deadlines met

At risk

2 of 3

DORA initial notification: sent 06:40 by Priya Anand, 25 min to spare (started 03:05).

Insurer notice: sent 08:30 by Elena Voss, 1 h 25 min late (started 03:05).

GDPR breach notification: sent 09:40 by Priya Anand, 66 h 50 min to spare (started 04:30).

Providers within contract

At risk

1 of 2

MDR provider: escalation to CoinExchange in 27 min against 30 min.

Incident response firm: responder on the bridge in 1 h 28 min against 1 h.

Systems within recovery target

At risk

2 of 3

dc01: back after 3 h 25 min against 4 h.

trade: back after 5 h 15 min against 6 h.

fs01: back after 7 h 40 min against 6 h. Online backup set deleted; restored from the offline copy.

Against targets

Deadlines

Time from the trigger to the notice, against each window. The line marks the deadline.

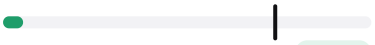
DORA initial notification — 3 h 35 min of 4 h

Sent 25 min early — Met

Insurer notice — 5 h 25 min of 4 h

Sent 1 h 25 min late — Late

GDPR breach notification — 5 h 10 min of 72 h



Sent 66 h 50 min early — Met

Providers

Elapsed time against the contracted time. The line marks the contract.

MDR provider: escalation to CoinExchange — 27 min of 30 min

3 min inside contract — Within

Incident response firm: responder on the bridge — 1 h 28 min of 1 h

28 min over contract — Late

Restores

Time down against each recovery target. The line marks the target.

Domain controller (dc01) — 3 h 25 min of 4 h

35 min inside target — Within

Trading platform (trade) — 5 h 15 min of 6 h

45 min inside target — Within

File server (fs01) — 7 h 40 min of 6 h

1 h 40 min past target — Late

Timeline

27 events

Key events

02:14 T+00:00 — Providers · MDR provider

EDR on fs01 flags a credential theft tool. The alert reaches the MDR provider and the escalation timer starts.

02:41 T+00:27 — Providers · MDR provider

Calls Mei Tan, CoinExchange's on-call analyst. Escalation took 27 minutes, inside the 30-minute contract.

02:47 T+00:33 — SOC · Mei Tan

Triages the alert in the SIEM and sees large outbound transfers from fs01.

02:58 T+00:44 — SOC · Rafa Lind

Escalates to the incident lead.

03:05 T+00:51 — Leadership · Ines Marlow

Declares a major incident. The DORA initial notification and insurer notice clocks start, and leadership is paged.

03:12 T+00:58 — Leadership · Ines Marlow

Calls the incident response firm. The retainer timer starts.

03:40 — Attacker · Attacker (operator)

T+01:26 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
T+01:38 SOC · Rafa Lind
Isolates the server segment and disables the VPN account j.berger.

04:05
T+01:51 Exercise control · Exercise control
Inject released: Leak site post

04:05
T+01:51 Exercise control · Exercise control
Inject released: Ransom note

04:30
T+02:16 SOC · Mei Tan
Confirms customer and employee records left fs01. The GDPR 72-hour clock starts.

04:40
T+02:26 Providers · Incident response firm
Responder joins the bridge 88 minutes after the call, outside the retainer's 60 minutes.

05:15
T+03:01 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
T+03:06 Exercise control · Exercise control
Inject released: Request for comment

05:25
T+03:11 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
T+03:16 IT operations · Sam Okafor
Black Start begins: restoring dc01 from backup.

05:40
T+03:26 Leadership · Jonah Albers
Decided: Publish the holding statement. Silence reads as hiding it once the post is public.

06:10
T+03:56 IT operations · Sam Okafor
The online backup set for fs01 was deleted by the attacker. Switching to the offline copy.

06:40
T+04:26 Leadership · Priya Anand
DORA initial notification sent: met with 25 min to spare.

07:05
T+04:51 IT operations · Sam Okafor
dc01 is back after 3 h 25 min, inside its 4-hour target.

07:05
T+04:51 Exercise control · Exercise control
The insurer notice deadline passed with nothing sent. Nobody owned it.

07:50 Leadership · Priya Anand

T+05:36		Decided: Send the initial notification now. We know enough to notify; waiting only risks the 24 hours.
08:30 T+06:16	Leadership · Elena Voss	Insurer notice sent: 1 h 25 min late.
08:55 T+06:41	IT operations · Sam Okafor	The trading platform is back after 5 h 15 min, inside its 6-hour target. Trading can resume.
09:40 T+07:26	Leadership · Priya Anand	GDPR breach notification sent: met with 66 h 50 min to spare.
11:20 T+09:06	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 T+09:16	Exercise control · Exercise control	Ends the drill. The after-action report and Readiness Record entry are drafted from the timeline.

Detections per attack step

2 of 5 attack steps raised an alert. The rest were found by people, or not at all.

Attack step	ATT&CK	Alert	Seen by	Response
Log in over the VPN as j.berger Initial access · vpn-gw	T1133 External Remote Services	No alert	Not seen	No alert; found by the SOC at 03:58
Run a credential theft tool on fs01 Credential access · fs01	T1003 OS Credential Dumping	Alert fired	EDR, then the MDR provider, at once	MDR provider escalated in 27 min
Stage files on fs01 and copy them out Exfiltration · fs01	T1041 Exfiltration Over C2 Channel	No alert	Mei Tan, in triage, after 25 min	No alert; seen in netflow at 02:47
Delete the online backup set for fs01 Impact · bkp01	T1490 Inhibit System Recovery	No alert	Sam Okafor, during restore	No alert; found at 06:10
Push ransomware through group policy from dc01 Impact · dc01	T1484.001 T1486 Group Policy Modification	Alert fired	Help desk and the SOC, after 6 min	Server segment isolated 12 min after encryption began

Decisions

05:15
T+03:01

The ransom demand

Decided by Tomas Reyna · authority: CEO, with general counsel

Pay | Open a negotiation | ✓ Refuse. Restore from backup

Reason: Backups for the systems that matter look intact, paying does not stop the leak, and counsel advises against it.

05:25
T+03:11

Restore order

Decided by Ines Marlow · authority: Incident lead

✓ dc01, then the trading platform, then fs01 | Trading platform first | fs01 first

Reason: Nothing else authenticates without dc01; trading is the business priority after that.

05:40
T+03:26

Public statement

Decided by Jonah Albers · authority: Head of communications

✓ Publish the holding statement | No comment yet

Reason: Silence reads as hiding it once the post is public.

07:50
T+05:36

DORA initial notification

Decided by Priya Anand · authority: General counsel

✓ Send the initial notification now | Wait for the forensic picture

Reason: We know enough to notify; waiting only risks the 24 hours.

Gaps

5 gaps, each with an owner

1 **No alert on the VPN to domain controller path, the same gap last month's attack test found**

Owner	Rafa Lind
Next step	Fix the detection, then retest in Attack Testing
Retest	Not scheduled

2 **No alert on the outbound transfer from fs01**

Owner	Rafa Lind
Next step	New detection, retested in the next attack test
Retest	Not scheduled

3 **The insurer notice has no owner in the incident response plan**

Owner	Priya Anand
Next step	Plan update, checked in the next Worst Day
Retest	Not scheduled

4 **Online backups for fs01 were reachable with domain credentials**

Owner	Sam Okafor
Next step	Separate the backup credentials, checked in the next Black Start
Retest	Not scheduled

5 **The incident response firm joined after its retainer time**

Owner	Ines Marlow
Next step	Raise with the firm; timed again in the next drill
Retest	Not scheduled

Review

What went well

- The MDR provider escalated inside its contract, and the SOC confirmed the theft within two hours.
- The SOC isolated the server segment 12 minutes after encryption began.
- Leadership refused the ransom with a recorded reason, and the restore order held all day.
- Both regulator notifications went out inside their windows: DORA with 25 minutes to spare, GDPR on the first day.

What could improve

- Detect the VPN to domain controller path the attack test found last month.
- Alert on large outbound transfers from fs01.
- Give the insurer notice an owner in the incident response plan.
- Keep backup credentials apart from domain credentials.
- Hold the incident response firm to its retainer time.

Where we got lucky

- The offline copy of fs01 was only six days old.
- The journalist's deadline came after the holding statement was ready.

Notes

The scenario clock ran from 02:14 to 11:30 scenario time, so the incident started overnight. Every time in this report is scenario time.

Exercise control played the attacker, the regulators, the insurer and the journalist. White cell moves are left out of this report.

Known differences between the copy and production

- Files on fs01 are generated samples with the same folder layout, sizes and permissions.
- The trading platform runs one application node; production runs three behind a load balancer.