1 WHAT STOPS TODAY, AND WHAT EXPOSURE DO WE BUY?

EXECUTIVE DECISION · AFTER INJECT 3 · TIMER 3 MINUTES

HELD BY **CIO**

VP R&D "Every day that link is dark, we lose ground we cannot win back." **CTO** "Every hour it stays open, the attacker can keep reading."

A **Dark now.** Research is paused on everything that depends on the link, and every way in is shut.

COST Financial one step worse. The Reputational step applies when Decision 3 resolves: this decision's triangle cannot shield it, Decision 3's can, and if Decision 3 expires it applies as a cost. **ROLL** Automatic if the owner of the old system was named in the first call, else 10+. **COMPLICATION** The shutdown breaks more of the link: Financial one more step.

B **A bounded window.** The link stays open under watch for one hour of story time, ending before inject 5, while a temporary link is built.

COST Security one step worse. **ROLL** 10+. **COMPLICATION** The attacker reads more research data in the window.

C **Wait for the temporary link, no limit.** The wait outcome if the time runs out.

COST Security two steps worse. **ROLL** 15+, it goes against the CTO's stated fact. **COMPLICATION** Security one step worse and Financial one step worse: the attacker finishes copying the most valuable data.

TRIANGLE TENSION Time (shut them out) against Money (protect research).

OPTION CHOSEN

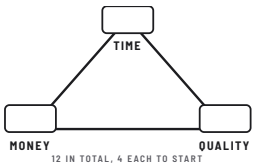
A B C NO RESOLUTION

VOTES

CEO ☐○ CFO ☐○ CIO ☐○ CISO ☐○ ☐○ ☐○

Square: for. Circle: against. Majority 3 of 4. A tie fails.

TRIANGLE, WRITTEN AS SET



ROLL, ONLY ON DOUBT

TARGET __+
ROLL __

BACKERS +1 ☐☐☐

SPECIALTY +___

At target: intended result. Within 3 below: partial, tell the complication. 4 or more below: failure, the complication moves the board.

WHAT IT LED TO, AND THE RISK BOARD AFTER

MALWARE & MANAGEMENT · OPERATION SILK HARVEST · DECISION CARD COUNTS AGAINST THE THREE EXECUTIVE DECISIONS DRAFT, WORKING ASSUMPTION

CUT

2 WHOSE TIME, AND WHAT EXPOSURE DO WE CARRY?

EXECUTIVE DECISION · AFTER INJECT 4 · TIMER 3 MINUTES

HELD BY **CFO**

CFO LINE, READ ONCE BY THE INCIDENT MASTER (IM) AT HALF TIME "Every day the integration team stays off integration costs us money and a week of slippage." **CTO** "We cannot certify the research environment clean for a day on our own."

A **Pull the integration team onto the response.** Certification takes hours, not a day.

COST Financial two steps worse. The integration work slips a week. **ROLL** Automatic, the CIO has clear ownership. **COMPLICATION** None.

B **Emergency budget and overtime; the integration work stays on schedule.** Certification takes about a day and a half.

COST Financial one step worse, in cash. **ROLL** 10+. **COMPLICATION** Reputational one step worse: overtime burns out the team and certification slips.

C **Run it with the internal team only.** Certification takes more than a day.

COST Reputational one step worse. **ROLL** 10+. **COMPLICATION** Reputational one step worse: a stakeholder calls the CEO before certification.

TRIANGLE TENSION Money against Time against Quality.

OPTION CHOSEN

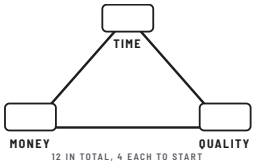
A B C NO RESOLUTION

VOTES

CEO ☐○ CFO ☐○ CIO ☐○ CISO ☐○ ☐○ ☐○

Square: for. Circle: against. Majority 3 of 4. A tie fails.

TRIANGLE, WRITTEN AS SET



ROLL, ONLY ON DOUBT

TARGET __+
ROLL __

BACKERS +1 ☐☐☐

SPECIALTY +___

At target: intended result. Within 3 below: partial, tell the complication. 4 or more below: failure, the complication moves the board.

CONSULTANT BOUGHT (3 OF 4 VOTE, ONCE, COST TO THE END OF THE SESSION) ☐

WHAT IT LED TO, AND THE RISK BOARD AFTER

MALWARE & MANAGEMENT · OPERATION SILK HARVEST · DECISION CARD COUNTS AGAINST THE THREE EXECUTIVE DECISIONS DRAFT, WORKING ASSUMPTION

3 WHAT DO WE SAY, TO WHOM, AND WHEN?

EXECUTIVE DECISION · AFTER INJECT 5 · ONE TIMER OF 3 MINUTES

HELD BY **CISO**

GENERAL COUNSEL "If we say nothing, the CSIRT will assume we are withholding. If we say too much, I cannot take it back." One stance, one vote, one roll. Lands cleanly only with a named CSIRT owner.

A **Open.** *CSIRT: full findings with stated confidence. Stakeholders: told now, calibrated. Supplier: formal demand.*

COST Financial one step worse. **ROLL** 10+. **COMPLICATION** Reputational one step worse: a later scope revision hurts credibility.

B **Measured.** *CSIRT: a validated subset. Stakeholders: told once scope is firmer. Supplier: ask for a call.*

COST Reputational one step worse. **ROLL** Automatic if a CSIRT owner is named and counsel confirmed what may be shared, else 10+. **COMPLICATION** Security one step worse: the subset omits something the CSIRT needs.

C **Hold.** *CSIRT: nothing yet, and it escalates its request. Stakeholders: told nothing.* The wait outcome.

COST Reputational two steps worse. **ROLL** 15+, counsel already said so.
COMPLICATION Reputational one step worse: the CSIRT escalates its request.

TRIANGLE TENSION Quality (a defensible account) against Time. A hybrid is recorded as a dissent, not a fourth option.

OPTION CHOSEN

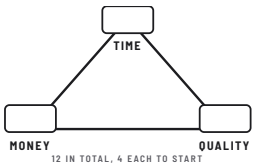
A B C NO RESOLUTION

VOTES

CEO □○ CFO □○ CIO □○ CISO □○ □○ □○

Square: for. Circle: against. Majority 3 of 4. A tie fails.

TRIANGLE, WRITTEN AS SET



ROLL, ONLY ON DOUBT

TARGET __+
ROLL __

BACKERS +1 □□□

SPECIALTY +___

At target: intended result. Within 3 below: partial, tell the complication. 4 or more below: failure, the complication moves the board.

WHAT IT LED TO, AND THE RISK BOARD AFTER

MALWARE & MANAGEMENT · OPERATION SILK HARVEST · DECISION CARD · COUNTS AGAINST THE THREE EXECUTIVE DECISIONS · DRAFT, WORKING ASSUMPTION

CUT

LC LEADERSHIP CALLS

THREE LEADERSHIP CALLS ON ONE CARD · NONE COUNTS AGAINST THE THREE

HELD BY **CEO**

1 THE FIRST CALL

Name the executive incident lead and the owner of the old system. No roll. Timer 1 minute. Without a name: the attacker reaches more research systems, Security one step worse, before Decision 1.

2 RESTART BEFORE CERTIFICATION?

Asked once while certification is pending. The table votes yes or no, 3 of 4. No CEO default. Yes accepts the technical team's stated risk. Roll 15+, it goes against the CTO's stated fact. Intended result: Financial one step better, not below Steady. Complication: a second way out is found late, Security one step worse.

3 WHO IS ACCOUNTABLE FOR FIXING WHAT THIS SHOWED, AND BY WHEN?

The CEO writes the remediation owner at the end. It is not a condition of containment.

VOTES, RESTART CALL

CEO □○ CFO □○ CIO □○ CISO □○ □○ □○

Square: for. Circle: against. Majority 3 of 4. A tie fails.

RESTART CALL

○ REOPEN ○ WAIT

ROLL, IF ANY, AND WHAT IT LED TO

MALWARE & MANAGEMENT · OPERATION SILK HARVEST · DECISION CARD · DOES NOT COUNT AGAINST THE THREE · DRAFT, WORKING ASSUMPTION