OPERATION SILK HARVEST

SCENARIO CARD · EXECUTIVE EDITION · BIOGENIX · SOURCE: THE WINNTI CARD

An attacker has been inside a life-sciences company for weeks, and the executives are told at one o'clock. This card gives you the story, the cast, the injects and the three Executive Decisions for a session of about an hour. It follows the rulings in the guide. Where a detail is open, it says so, and you rule.

FROM SOURCE CARD CARRIED FROM THE VANILLA WINNTI CARD IN PLAIN BUSINESS WORDS

NEW FOR THIS CARD OR ASSUMED WRITTEN FOR THIS CARD, NOT RULED RULED DECIDED BY THE GAME'S AUTHOR

SESSION
ABOUT AN HOUR
Four executives. The technical team works off-screen. RULED

SEATS
CEO, CFO, CIO, CISO
Four NPCs you play: General Counsel, Head of Communications, COO, Chief Risk Officer. RULED The CTO and VP R&D are off-screen characters you voice.

EXECUTIVE DECISIONS
UP TO 3
Menus fixed by this card. RULED All three are played in a session of about an hour. ASSUMED

RISKS THAT LEAD
FINANCIAL, REPUTATIONAL
Security always counts. The IM reads the priority from this card. RULED

REGULATORY MARKER
POSSIBLE DUTY, OPEN
A marker, not a fourth risk. No deadline is asserted; General Counsel is assessing.

STATUS
DRAFT, NOT PLAYED
Built from the Winnti card. Nothing here is playtested or timed. ASSUMED

READ ALOUD AT THE START NEW FOR THIS CARD

> *A national CSIRT called your CISO a couple of hours ago with a warning about a campaign against life-sciences companies. BioGenix has seen Chinese threat actors in its network before. That is all the record says. Your technical team has been checking since. At five to one they found that you are part of it. Here is your first brief. You are the executive team. The technical team will tell you what it finds. You decide what it is allowed to do, what it may spend and what you are prepared to say.*

FROM SOURCE CARD The hook: it is Thursday, 13:00. The CISO's first line to the teams in the source card is "we do not yet know if we are compromised". Here your technical team has found out that you are. What you cannot afford is to be the last to know.

THE COMPANY AND WHAT IS AT STAKE

FROM SOURCE CARD **BioGenix** is a life-sciences company built on a precision-fermentation platform. Its crown jewel is **GenixLibrary**, three years of proprietary genomic sequence research. It recently merged with another firm and is still integrating infrastructure. Active fermentation projects depend on the library.

THE LESSON BEHIND THE OPENING
Nobody inside BioGenix saw this for three to four weeks. It was the warning from outside that turned it up.

RULED **Table rule for this card:** the table never sees technical artifacts such as logs, scans, certificates or tool names. Everything it sees is business language and management exhibits. Plain words such as "system" or "research cloud" are fine; never state jargon or say "this is a supply chain compromise". NEW FOR THIS CARD

THE ESCALATION CARD

RULED The Escalation Card has a severity cell and a page rule. Put it on the table with the first brief, so the table can see why it is called now. The routing rule is an illustration of how a firm might route, not a claim about every firm. NEW FOR THIS CARD

IMPACT, HIGH AT TOP	LOWER URGENCY	HIGHER URGENCY
High impact	ASSESS	CONVENE THIS INCIDENT
Lower impact	WATCH	ASSESS

THIS INCIDENT: HIGH IMPACT AND HIGH URGENCY. A CROWN-JEWEL SYSTEM, WITH CREDIBLE SPREAD OR DATA LOSS.

- **Page rule.** The technical lead and the CISO assess. When the cell reaches HIGH, or a decision exceeds their authority (spend, disrupting research, speaking outside), the executive incident lead convenes the executives and counsel. Board notification is a separate step and is not played.
- **What crossed the line, and when.** The call from the CSIRT was about two hours earlier, at about 11:00. At 12:55 the technical team confirmed that an attacker is inside, with data probably gone. The way in stays ask-gated. They escalated within minutes. The executives sit at 13:00. NEW FOR THIS CARD This follows the source card, which says "a couple of hours": the executives are called at the finding, not at the warning.
- **Open question for the table.** Is any legal or notification duty possible? General Counsel raises it as an assessment in progress. No deadline is asserted.
- **"Why were we called now?"** The table may ask once, for 30 seconds. Answer: the finding that justified it came five minutes ago, about two hours after the call, and the attacker has been in for weeks. Longer discussion is banked to the debrief.

THE BRIEF
The rulings fix one full brief at the start, then short briefs at each inject. RULED A short brief has three lines: what changed, what is new and unknown, the new deadline. The CISO player gives the table a 30-second decision summary, and the CTO, voiced by you, supplies the facts.

A FULL BRIEF HAS SEVEN FIELDS
1. What happened and the business impact, in one sentence. 2. What we know and what we do not, each tagged Confirmed, Probable or Unknown, with its basis, an "as of" time and, for each Unknown, what would change it. 3. What the technical team is doing now. 4. The decision: two or three options, each trade-off, the team's recommendation, whether it can be reversed, and what happens if the table waits. 5. Who the table proposes to own it, and by when; the table assigns the owner. 6. Any open legal or notification question. 7. Next update time.

ASSUMED Time budget: the first brief and escalation card 2 minutes, each short brief 20 seconds, the challenge 30 seconds, five minutes in total. If a run goes long, shorten the short briefs. A brief carries what a decision needs and never explains why it happened: causes stay Unknown until a player asks. Before a vote the CISO states one sentence: "we are deciding X because we know Y and do not know Z". If it is missing, wait for it; do not refuse the vote. ASSUMED **Opening round, 60 seconds, after the read-aloud and the brief.** In seat order (CEO, CFO, CIO, CISO), one sentence each, written on the seat card, never scored, no debate. Say: "Speaking as your seat, with your own judgment: state the one risk this warning creates for BioGenix that your seat owns. Say it as 'if this happens, then that', in your own words, not as a category." If an answer is a category word, is generic or is about last time, say once: "Say it as if-then, for BioGenix, today." The debrief lays each line beside the seat's votes: did the decisions reduce that risk, accept it or trade it for another?

THE CAST

CEO
SEAT, VOTES
Owns the call on stakeholder accountability and what the firm is prepared to say.

CFO
SEAT, VOTES
Carries the cost of a halted fermentation week and of any outside help.

CIO
SEAT, VOTES
Containment happens in IT. The CTO reports here.

CISO
SEAT, VOTES
Took the CSIRT call. Gives the 30-second summary before each vote.

CTO
VOICED BY YOU FROM SOURCE CARD
Wants to cut the door shut and keep the evidence. The voice of the off-screen team. The source card gives evidence preservation to the CISO; here the CTO carries it too. NEW FOR THIS CARD

VP RESEARCH AND DEVELOPMENT
VOICED BY YOU FROM SOURCE CARD
"Three years of my team's work is on that network." Protects research continuity.

GENERAL COUNSEL
NPC NEW FOR THIS CARD
Will not let anyone say "not notifiable" yet. Evidence, privilege, who may be told what.

HEAD OF COMMUNICATIONS
NPC NEW FOR THIS CARD
Wants a position, not certainty. Stakeholders, the press, a defensible account.

RULED The other NPCs are General Counsel, Head of Communications, COO and Chief Risk Officer. They give facts, advice, questions and pressure, and never vote, decide or roll. A fifth to eighth player converts an NPC into a seat with one vote, in this order: General Counsel, Head of Communications, COO, Chief Risk Officer. A converted seat has no specialty strengths. A decision passes by strict majority: 3 of 4, 3 of 5, 4 of 6, 4 of 7, 5 of 8. A tie fails. NEW FOR THIS CARD The CTO and the VP R&D come from the source card; you voice them as the technical team and research leadership. They are never seats. This card uses General Counsel and Head of Communications most.

THE HOUR

9 min	7 min	8 min	7 min	10 min	15 min
OPENING AND FIRST CALL	**EXECUTIVE DECISION 1**	**INJECT 4, DECISION 2**	**INJECT 5, DECISION 3**	**QUESTIONS AND BUFFER**	**VERDICT, DEBRIEF**
Escalation Card, the one full brief, read-aloud, opening risk round, rules in 90 seconds, the first call	Inject 3, the Rules Card for the triangle and roll, timer, vote, narrate	Short brief, the CTO's estimate, restart vote, the consultant offer	Short brief, the CSIRT's request, timer, vote, narrate	Three question windows and slack for the Financial-Critical board call	The two-part verdict, then the debrief

ASSUMED This is a plan for a workshop slot of about an hour, 56 minutes on paper plus about 4 minutes of float. It is arithmetic, never played. The game itself has no hard stop: your IM decides whether and when to call time. Inject times such as 13:00 are story time, not table minutes. The three-act shape: Act 1 sets up why now and who has skin in the game; Act 2 escalates, and things worsen the longer the table waits; Act 3 is the climax and the verdict, then the debrief. If a run goes long, cut in this order: the consultant offer, Exhibit B (show it in the debrief), the false lead, then merge Decisions 1 and 2. A fourth Executive Decision is never added.

THE INJECTS

Each inject arrives as a person who wants something, carries a price and a deadline, and ends in a question to a seat. Inject 2 of the source card is merged into inject 1, so the deck is numbered 1, 3, 4, 5, 6. One full brief at the start, then a short brief at each inject. NEW FOR THIS CARD

1 THE OLD SYSTEM

STORY CLOCK 13:00

HEARS An old system that was supposed to be switched off has been sending your research data out. The technical team can prove an attacker is using it. Cutting it off will also cut a research collaboration link, and the CTO needs a name. FROM SOURCE CARD

ASK-GATED "How did they get in?" or "What did we agree with the supplier?" CTO: "Through software from one of our suppliers. Ask General Counsel what we agreed with them." (Exhibit A.) "Why is it still on?", "Who owns it?", or the VP R&D's "IT says it's in maintenance" followed by "check it": CTO: "That record says switching it off was postponed to keep research running. It says: the owner has since left, no handover." (Exhibit B.) If nobody has asked by the end of the first question window, ask one seat: "CFO, what do you want to know before you decide?"

THE FIRST CALL A leadership call, not an Executive Decision: the CEO names the executive incident lead, the owner of the old system and the contact for the CSIRT. Anyone may object, which forces a 3-of-4 vote. No roll, a one-minute timer, and it does not count against the three decisions. RULED If nobody is named, the attacker reaches more research systems: Security one step worse before Decision 1. ASSUMED

FALSE LEAD The VP R&D says "IT says that system is in maintenance." The record is really a decommissioning blocker. The table can ask the CTO to check. FROM SOURCE CARD

3 THE PRICE OF THE LINK

STORY CLOCK 13:30, INSIDE DECISION 1

HEARS The attacker also holds an open door into your research environment, left over from the old arrangement. The CTO can shut every way in within the hour, but the research collaboration link goes dark with it. FROM SOURCE CARD

TWO PRICES VP R&D: "Every day that link is dark, we lose ground we cannot win back, and our stakeholders will ask why." CTO: "Every hour it stays open, the attacker can keep reading." The table is asked how long research may be exposed, and how long it may be dark.

FALSE LEAD The research lead's comfort: "It's probably just the quarterly refresh." It is a bias trap: that project is documented and separate, and the data is going somewhere new.

THEN Call Executive Decision 1.

4 THE COST AND THE CLOCK

STORY CLOCK 14:00, DECISION 2

HEARS Core research data has been leaving for weeks, in small quantities that looked routine and that nothing flagged. FROM SOURCE CARD

NPC CTO: "My team cannot put its hand on its heart that the research environment is clean for at least a day on our own." General Counsel: "Whether this triggers a duty to notify anyone depends on our sector and jurisdiction. I will have an assessment before you speak to stakeholders. Do not call this 'not notifiable' until I do."

TABLE QUESTION Whose time, and what exposure: certification is much faster if the integration team is pulled off integration, but the integration work slips. If Decision 1 cut the system off, the leaking has stopped and the CTO says so, but still cannot promise there is no other way out. If not, the CTO says more is leaving now.

THEN Call Executive Decision 2. Inside its timer: the restart vote and the consultant offer.

5 IT IS A CAMPAIGN

STORY CLOCK 14:30, DECISION 3

HEARS The CSIRT confirms at least three other life-sciences victims in six months and asks BioGenix for its findings so it can warn others. FROM SOURCE CARD

TENSION Sharing helps the sector, but the findings expose BioGenix's own weaknesses, recovery work competes for the same people.

RED FLAG No single owner for CSIRT coordination. FROM SOURCE CARD

THEN Call Executive Decision 3. At the end of play the CEO writes one name in the Decision Record: who is accountable for fixing what this showed, and by when. It is not a condition of containment.

6 THE PIVOT

STORY CLOCK 15:00

HEARS Only what the table actually achieved, narrated by you in two sentences: the ways in that were shut, whether the leaking has stopped, and what is still open.

CONTAINMENT You declare it. RULED You declare it only after Decision 3 has resolved. This card's test: two marks are set, Ways in shut and Leak stopped; they are necessary, not sufficient. ASSUMED If they are not when you call time, the verdict says "not yet reached" and the cost sentence is read.

EXECUTIVE DECISIONS

TIMER ADDS PRESSURE
Deciding under pressure is a skill, and a real incident does not wait for consensus. A visible timer runs for every Executive Decision. RULED Its length is yours to set; this card uses 3 minutes. IM RULING SPACE

- The timer covers deliberation only: NPC questions (at most two, one-line answers), one sentence of position from each seat, the triangle allocation, the CISO's one sentence and the vote. It pauses while you read the brief or narrate.
- Each executive speaks once, one sentence, in turn. Call half time once, and the vote with about a minute left. Votes are cast together.
- A tie fails. The table may re-propose once while time remains. A vote in progress at expiry is completed.
- If the timer runs out with no majority, say "no resolution" aloud. The decision is spent and counts against the three, and the wait option applies automatically with its cost and its complication, unrolled and unshielded, with no vote. RULED Choosing to wait on purpose is the same option and needs a majority as usual.
- Before each vote the CISO states one sentence: "we are deciding X because we know Y and do not know Z".

ASSUMED All durations are untested. The timer is a pacing tool, not a score. In the debrief ask what the pressure did to each decision, and what the table would have decided with ten more minutes.

THE THREE EXECUTIVE DECISIONS

RULED The menus are fixed by this card. NEW FOR THIS CARD A "+1" is one step worse on the risk board; the costs, roll targets and complications are printed on the option cards, so you never judge difficulty on the day. For each decision: read its brief, start the timer, let the table set the triangle and vote, roll only if the outcome is in doubt, then narrate and move the board.

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

TIMER: 3 MINUTES

Held by the CIO. The technical team keeps a copy of the evidence in every option; the table decides how long research stays dark or exposed. NEW FOR THIS CARD

(A) Dark now. Research is paused today on everything that depends on the link, and the technical team shuts every way in.
COST ON THE BOARD Financial +1 now; Reputational +1 when Decision 3 resolves, unless Decision 3 is Open
ROLL TARGET none if an owner was named in the first call, else 10+
COMPLICATION Financial +1 (the shutdown breaks more of the link)

(B) A bounded exposure window. The link stays open under watch for one hour of story time, ending before inject 5, while the technical team builds a temporary link.
COST ON THE BOARD Security +1
ROLL TARGET 10+
COMPLICATION Security +1 (the attacker reads more research data)

(C) Wait for the temporary link, no limit. On the menu because real teams choose it to protect research. WAIT OPTION
COST ON THE BOARD Security +2
ROLL TARGET 15+, it goes against the CTO's stated fact
COMPLICATION Security +1 and Financial +1 (the attacker finishes copying the most valuable data)

TRIANGLE TENSION Time (shut them out) against Money (protect research continuity).
MEANWHILE At half time CTO: "The attacker still has a door into the research environment while you talk." VP R&D: "Every day that link is dark, we lose ground we cannot win back."

2 WHOSE TIME, AND WHAT EXPOSURE DO WE CARRY?

TIMER: 3 MINUTES

Held by the CFO. Inside this timer sit the restart vote and the consultant offer. NEW FOR THIS CARD

(A) Pull the integration team off integration and onto the response. Certification takes hours, not a day.
COST ON THE BOARD Financial +2, and the integration work slips a week
ROLL TARGET none, the CIO has clear ownership
COMPLICATION none

(B) Authorise emergency budget and overtime and keep the integration work on schedule. Certification takes about a day and a half.
COST ON THE BOARD Financial +1
ROLL TARGET 10+
COMPLICATION Reputational +1 (overtime burns out the team and certification slips)

(C) Run it with the internal team only. Certification takes more than a day; the research environment stays offline longer. WAIT OPTION
COST ON THE BOARD Reputational +1
ROLL TARGET 10+
COMPLICATION Reputational +1 (a stakeholder calls the CEO before certification)

RESTART BEFORE CERTIFICATION A leadership call, voted 3 of 4, not counted against the three decisions. "Do you reopen research before it is certified?" Yes accepts the technical team's stated risk. Roll target 15+; if it lands, Financial one step better (not below Steady); complication Security +1. ASSUMED
MEANWHILE At half time the IM reads the CFO's line: "Every day the integration team stays off integration costs us money and a week of slippage." CTO: "I cannot certify the research environment is clean for at least a day on our own."

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

TIMER: 3 MINUTES

Held by the CISO, who speaks for the CSIRT; General Counsel gates what may be shared. One stance, one vote, one roll. NEW FOR THIS CARD

(A) Open. Share the findings with the CSIRT now with stated confidence, tell stakeholders now with a calibrated statement, and send the supplier a formal demand for an explanation.
COST ON THE BOARD Financial +1
ROLL TARGET 10+
COMPLICATION Reputational +1 (a later scope revision hurts credibility)

(B) Measured. Share a validated subset with the CSIRT, tell stakeholders once the scope is firmer, and ask the supplier for a call.
COST ON THE BOARD Reputational +1
ROLL TARGET none if the CSIRT contact was named in the first call and General Counsel confirmed what may be shared, else 10+
COMPLICATION Security +1 (the subset omits something the CSIRT needed)

(C) Hold. Say nothing until the investigation completes. WAIT OPTION
COST ON THE BOARD Reputational +2
ROLL TARGET 15+, General Counsel already said the CSIRT will assume BioGenix is withholding
COMPLICATION Reputational +1 (the CSIRT escalates its request)

MEANWHILE At half time General Counsel: "If we say nothing, the CSIRT will assume we are withholding. If we say too much, I cannot take it back." A table that wants a hybrid records it as a dissent on the card; it is not a menu item.

SECRETS AND EXHIBITS

The layers are for the debrief. Never state them. The table meets them only as management documents and people's words, handed over when a player asks. If a table never asks, do not give: show the exhibits in the debrief and ask what they say. NEW FOR THIS CARD

A — SURFACE SECRET
FAST-TRACK EXCEPTION
BioGenix let a supplier's software in under a fast-track exception and never checked it independently.
EXHIBIT A
The supplier fast-track exception record. Give it when someone asks "how did they get in?" or "what did we agree with the supplier?".

B — DEEPER SECRET
NOBODY OWNED THE TRADE-OFF
An old system stayed on the network for 18 months because a research link depended on it, and nobody owned that call.
EXHIBIT B
The integration steering minutes: "keep the research link alive until migration completes; decommissioning deferred, the owner has since left, no handover". Give it when someone asks "why is that system still on?" or "who owns it?".

C — ROOT SECRET
SPEED AGAIN AND AGAIN
In the months after the merger, speed and continuity were chosen again and again, and no executive owned the accumulated risk.
EXHIBIT C
The record that the switch-off was deferred, with the owner gone and no handover. Debrief only, or if someone asks "was this the only one?".

The root layer is not reachable within the timers. The project owner's note and the CSIRT's request are not secret exhibits. The debrief steers to the organisation's decision record, never to blaming a player.

THE PANIC-HIRED CONSULTANT

RULED After the CTO's estimate at inject 4 the table may buy outside help, once, inside Decision 2's timer, by majority vote. It is not one of the three Executive Decisions. Before the vote, read the cost aloud, flat: "a new, uncontracted emergency engagement; it cannot contribute inside this window."

CONDITION · HURTS
PANIC-HIRED CONSULTANT
Financial one step worse from purchase to the end of the session. No countdown, no benefit. The triangle is untouched, and Money cannot shield it away.
NO COUNTDOWN RULED

NARRATION
WHY IT HURTS
Help bought in the middle of an incident cannot onboard inside the window. If nobody buys it, that is a defensible call and debrief material: "who was tempted, and when?" Never bait a purchase through urgency.

RULES THIS CARD ASSUMES

The mechanics themselves are ruled in the guide. These are the working defaults this card runs on, so you can run it. Each can change without touching the story, and the IM can rule differently. IM RULING SPACE

RISK TRIANGLE RULED	Money protects Financial, Time protects Security, Quality protects Reputational. An arm at 7 or more cancels one step of a printed cost on its paired risk; an arm at 2 or less adds one step to it, once per decision. Every shield costs a starve. The triangle returns to 4, 4, 4 after each decision.
PRINTED COSTS RULED	A printed cost applies on every outcome. Shields cancel printed cost steps only, never complications.
PARTIAL AND FAILURE RULED	A partial result (within 3 below the target) gives the intended outcome plus the option's complication told as a story beat, as in vanilla, with no board move. A failure (4 or more below) moves the board by the complication in full and delays the outcome. ASSUMED The delay is one decision; after Decision 3 the table reads the outcome in the debrief.
BACKERS RULED	Each other seat that backs the option with a concrete commitment adds +1 to the roll, up to +3.
SPECIALTY RULED	Each seat has three strengths on its role card, graded +3, +2 and +1, as in vanilla. The seat that proposed the carried option adds the one that fits. It stacks with backing. ASSUMED The grades are defaults. Option cards do not name a specialist seat; you rule it on the day.
CONTAINMENT TEST ASSUMED	Two marks on the board, Ways in shut and Leak stopped, set by Decision 1. You declare containment after Decision 3 has resolved, and only when both are set. A table that finishes early fills the Decision Record. The remediation owner is not a condition.
CRITICAL RISK RULED	A risk that reaches Critical is announced at once with a concrete symptom. Financial at Critical triggers one forced beat: an emergency board call, one sentence from each executive, and play runs on.

CLOSE AND DEBRIEF

RULED Close with the two-part verdict, not a score: whether containment was reached, or not yet reached if you called time first, and one sentence on the cost read off the risk board. If a risk is at Critical, say so. Then debrief as a guide, never a judge. The plan allows about 13 minutes. ASSUMED

- **Out of character, 3 min.** "Let's step out of the room for a moment." A 30-second check-in: "How was that clock?"
- **Reveal, 3 min.** Lay out Exhibits A, B and C and the real timeline. "What happened", never "what went wrong".
- **Each seat, 3 min.** Each seat speaks once: "Did your decisions reduce the risk you named at the start, accept it or trade it for another, and which decision did the clock change?"
- **Process gaps, 2 min.** "Who owned the old system in your organisation?" "Which decision should have been prepared before this meeting?" "Who else outside the room needed to know: the board, the CSIRT, the stakeholders?" Why did "it's just the refresh" feel convincing?
- **The Decision Record, 2 min.** Fill in the Decision Record sheet, or lay the decision cards out in order beside it: an incident name, the decisions taken and what each cost, the secrets found and missed, the verdict, and one "when X, I will Y" per player with a deadline. The CEO writes the remediation owner.

WHAT THE IM MUST NOT DO

- ✖ Describe technical detail the table must act on.
- ✖ Decide for the table.
- ✖ Let an NPC vote or choose.
- ✖ Adjust a roll for a nicer story.
- ✖ Declare containment before the last Executive Decision has resolved, or before both marks are set.
- ✖ Steer the debrief to blaming a player.

Draft. Derived from the vanilla Winnti scenario card (BioGenix), script v0.35 and card texts v0.2. Not playtested, not timed. The mechanics come from `core/rulings.md`.