# RULES CARD

MALWARE & MANAGEMENT · READ ONCE, KEEP ON THE TABLE

1

## OBJECTIVE

Contain a fast-moving malware incident by resourcing, authorising and defending your technical team's response, before it spreads and before the business pays more than it can afford.

2

## EXECUTIVES DECIDE

You always decide. Your Incident Master (IM) rolls a d20 only in doubt, against the target on the option card. Backers add +1 each, up to +3, and the proposing seat adds its specialty, +1 to +3.

3

## THREE RISKS

Security, Financial and Reputational risk sit on a board for everyone to see. The scenario card says which matters most. Time is the clock, not a risk.

4

## EXECUTIVE DECISIONS

Big calls are Executive Decisions: at most 3 per game, from the menu on the scenario card. A strict majority carries it: 3 of 4, 3 of 5, 4 of 6, 4 of 7, 5 of 8 seats. A tie fails. The IM chairs.

5

## RISK TRIANGLE

12 points: Money, Time and Quality, 4 each. A point is what you protect: Money the budget, Time speed, Quality thoroughness. Money pairs with Financial, Time with Security, Quality with Reputational: 7 or more shields a step, 2 or less adds one.

6

## TIMER ADDS PRESSURE

Every Executive Decision runs against a timer, because real incidents do not wait for consensus. Your IM sets the length.

7

## LASTING EFFECTS

A condition is a card for a lasting effect, tracked by your IM. Some help, some hurt. The panic-hired consultant only costs: bought at most once, inside Decision 2, it makes Financial Risk one step worse to the end of the session, and money cannot shield it away.

8

## HOW IT ENDS

Your IM declares containment after the last Executive Decision, and the game ends there. There is no score: the verdict says whether containment was reached and what it cost. If time runs out, your IM calls it. Anything this card does not settle, your IM rules.

CUT

# ESCALATION CARD

OPERATION SILK HARVEST · WHY YOU ARE CALLED NOW

### SEVERITY CELL

| IMPACT, HIGH AT TOP | LOWER URGENCY | HIGHER URGENCY |
|---|---|---|
| | ASSESS | **CONVENE** THIS INCIDENT |
| | WATCH | ASSESS |

HIGH IMPACT ON 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

| | |
|---|---|
| **~11:00** | The national CSIRT calls the CISO with a warning. |
| **12:55** | The technical team confirms an attacker is inside, with data probably gone. |
| **13:00** | You sit down. The way in is yours to ask about. |

### OPEN LEGAL QUESTION

General Counsel: "I am assessing whether any duty to notify applies. No deadline yet."

# EXECUTIVE SITUATION BRIEF

BRIEF NO. ____ · AS OF ____:____

**CISO, 30 SECONDS, BEFORE ANY VOTE**

"We are deciding _____ because we know _____ and do not know _____."

## 1 WHAT HAPPENED, AND THE BUSINESS IMPACT one sentence

## 2 WHAT WE KNOW AND WHAT WE DO NOT tag each item; an Unknown says what would change it

| ITEM | TAG | BASIS AND AS-OF TIME | WHAT WOULD CHANGE IT |
|---|---|---|---|
| | ◯ Conf ◯ Prob ◯ Unkn | | |
| | ◯ Conf ◯ Prob ◯ Unkn | | |
| | ◯ Conf ◯ Prob ◯ Unkn | | |
| | ◯ Conf ◯ Prob ◯ Unkn | | |
| | ◯ Conf ◯ Prob ◯ Unkn | | |

## 3 WHAT THE TECHNICAL TEAM IS DOING NOW

## 4 THE DECISION two or three options

**OPTION A**
Trade-off. Reversible?

**OPTION B**
Trade-off. Reversible?

**OPTION C**
Trade-off. Reversible?

THE TECHNICAL TEAM RECOMMENDS

IF WE WAIT: BY WHEN, AND WHAT GETS WORSE

## 5 PROPOSED OWNER AND DEADLINE the table assigns the owner

## 6 OPEN LEGAL OR NOTIFICATION QUESTION

## 7 NEXT UPDATE AT

# SHORT BRIEF

OPERATION SILK HARVEST · ____:____

WHAT CHANGED

NEW, AND WHAT WE DO NOT KNOW

NEW DEADLINE, AND WHO OWNS IT

ABOUT 20 SECONDS. READ IT OUT, THEN ASK THE SEAT THE QUESTION.

SHORT BRIEF SLIP · DRAFT

CUT

# SHORT BRIEF

OPERATION SILK HARVEST · ____:____

WHAT CHANGED

NEW, AND WHAT WE DO NOT KNOW

NEW DEADLINE, AND WHO OWNS IT

ABOUT 20 SECONDS. READ IT OUT, THEN ASK THE SEAT THE QUESTION.

SHORT BRIEF SLIP · DRAFT

CONDITION · HURTS — LASTS TO THE END

## PANIC-HIRED CONSULTANT

Financial Risk is one step worse from the moment it is bought to the end of the session. No countdown, no benefit. The triangle is not touched, and Money cannot shield it away. Bought at most once, inside Decision 2, by majority vote.

BOUGHT

Tick the Decision 2 card

MALWARE & MANAGEMENT — CONDITION CARD

CONDITION · HELPS — EXAMPLE

## REPUTATION SHIELD

An example of a helpful condition: cancels one step on Reputational, until the next Executive Decision resolves. Your IM may change its effect and its length.

COUNTDOWN (your IM sets how long and ticks off)

1 2 3 4 5

MALWARE & MANAGEMENT — CONDITION CARD

CONDITION · HELPS — BLANK

COUNTDOWN (your IM sets how long and ticks off)

1 2 3 4 5

MALWARE & MANAGEMENT — CONDITION CARD

CONDITION · HURTS — BLANK

COUNTDOWN (your IM sets how long and ticks off)

1 2 3 4 5

MALWARE & MANAGEMENT — CONDITION CARD

# RISK BOARD

MALWARE & MANAGEMENT · THE IM MOVES THE MARKERS ALOUD AFTER EACH DECISION

| | STEADY | STRAINED | SERIOUS | CRITICAL |
|---|---|---|---|---|
| **SECURITY** Is the attacker still in, and how far can they reach? |  |  |  |  |
| **FINANCIAL** What the response is costing, and what the business can afford. |  |  |  |  |
| **REPUTATIONAL** Trust with stakeholders, the CSIRT and the public. |  |  |  |  |

### HOW THE BOARD WORKS

- Every risk starts at Steady. "One step worse" moves a marker one step toward Critical.
- The IM moves a marker aloud after each decision and says why.
- A risk that reaches Critical is announced at once, with something the table can see, for example "the attacker has reached a new system". It is never banked silently.
- Financial at Critical triggers one emergency board call: each executive answers in one sentence, and play runs on.

### THE CLOSING VERDICT, READ OFF THIS BOARD

- **Containment:** reached, or not yet reached if your IM calls time first.
- **The cost:** one sentence, for example "Security Steady, Financial Serious, Reputational Strained". If contained with any risk at Critical: "contained, at a cost the business cannot sustain".

SECURITY _____ FINANCIAL _____ REPUTATIONAL _____