

TECH LENS · EXPLOITABILITY

NATION STATE



READS LIKELIHOOD

They have already done the reconnaissance. Assume they know your exposed services and your patch lag. Time is on their side.

STEER

Lean one rung higher if the actor in your seeded game already had a foothold, or any internet-facing system is behind on patches.

Reveal by saying it in your own words, not by showing the card.

RISK DECK

TECH LENS · EXPLOITABILITY

ORGANIZED CRIME



READS LIKELIHOOD

Money is the motive, so they automate and hit the same weakness across everyone, you included.

STEER

Lean one rung higher if your seeded incident used a commodity or known-CVE entry, or you run a common off-the-shelf stack.

Reveal by saying it in your own words, not by showing the card.

RISK DECK

TECH LENS · EXPLOITABILITY

INSIDER



READS LIKELIHOOD

The access is already inside the perimeter. Controls that assume an outside attacker do not even see this.

STEER

Lean higher if your seeded detection was perimeter-focused; lower if least-privilege and internal logging caught movement.

Reveal by saying it in your own words, not by showing the card.

RISK DECK

TECH LENS · EXPLOITABILITY

HACKTIVIST



READS LIKELIHOOD

Driven by a cause and a deadline. Capability is moderate, but motivation spikes around a trigger like a news event or campaign.

STEER

Lean higher if the org was in the news or tied to a contested issue at the time of the seeded incident.

Reveal by saying it in your own words, not by showing the card.

RISK DECK

TECH LENS · EXPLOITABILITY

OPPORTUNIST



READS LIKELIHOOD

Uses known exploits and public tooling. Stopped cold by basic hygiene, devastating wherever hygiene lapsed.

STEER

Lean lower if patching and MFA held in the seeded game; higher if a default credential or unpatched edge device was the way in.

Reveal by saying it in your own words, not by showing the card.

RISK DECK

BUSINESS LENS · BLAST RADIUS

CUSTOMER PRIVATE DATA



READS IMPACT

Not just cleanup. A breach here triggers notification duties, regulator attention, and customer churn that outlasts the incident.

STEER

Lean one tier higher if the seeded data is regulated or personal.

Reveal by saying it in your own words, not by showing the card.

RISK DECK

BUSINESS LENS · BLAST RADIUS

CORE PRODUCTION SYSTEM



READS IMPACT

Every hour down is revenue not earned and contracts at risk. The cost is per-hour and compounding, not a one-time hit.

STEER

Read the band as cost-per-hour times how long the seeded outage would realistically run.

Reveal by saying it in your own words, not by showing the card.

RISK DECK

BUSINESS LENS · BLAST RADIUS

FINANCIAL RECORDS



READS IMPACT

If numbers are quietly altered and the business acts on them, the damage is decisions made on false data and found late.

STEER

Lean one tier higher if the business would act on the seeded data before anyone noticed.

Reveal by saying it in your own words, not by showing the card.

RISK DECK

BUSINESS LENS · BLAST RADIUS

SOURCE CODE & IP



READS IMPACT

Losing this hands a competitor years of work and can void what makes the product defensible.

STEER

Lean one tier higher if the seeded asset embeds secrets or keys, or is the core differentiator.

Reveal by saying it in your own words, not by showing the card.

RISK DECK

So, tell me...

what's the worst thing
that could happen?



RISK DECK

· CLUE ·

So, tell me...

what's the worst thing
that could happen?



RISK DECK

· CLUE ·

So, tell me...

what's the worst thing
that could happen?



RISK DECK

· CLUE ·

So, tell me...

what's the worst thing
that could happen?



RISK DECK

· CLUE ·

So, tell me...

what's the worst thing
that could happen?



RISK DECK

· CLUE ·

So, tell me...

what's the worst thing
that could happen?



RISK DECK

· CLUE ·

So, tell me...

what's the worst thing
that could happen?



RISK DECK

· CLUE ·

So, tell me...

what's the worst thing
that could happen?



RISK DECK

· CLUE ·

So, tell me...

what's the worst thing
that could happen?



RISK DECK

· CLUE ·

BUSINESS LENS · BLAST RADIUS

BACKUPS

CLUE

READS IMPACT

If the backups are hit, recovery time turns into recovery hope. This is the line between an incident and a catastrophe.

STEER

Lean one tier higher if backups were online or reachable from the same network as production.

Reveal by saying it in your own words, not by showing the card.

RISK DECK

YOUR LENS

TECH LENS

LENS

YOU READ LIKELIHOOD

Your clue shows how the attacker operates and how likely they are to succeed here.

You own the Likelihood call.

EACH ROUND

1. Beat 1: privately commit your read AND a blind guess of a Business-Lens player.

2. Beat 2: reveal your clue by saying it plain, then re-commit together.

3. On a Boardroom answer from your Lens, a neighbour may only coach "help me say it better."

Commit before you reveal. Always.

RISK DECK

YOUR LENS

BUSINESS LENS

LENS

YOU READ IMPACT

Your clue shows what the business actually loses and how bad it gets.

You own the Impact call.

EACH ROUND

1. Beat 1: privately commit your read AND a blind guess of a Tech-Lens player.

2. Beat 2: reveal your clue by saying it plain, then re-commit together.

3. On a Boardroom answer from your Lens, a neighbour may only coach "help me say it better."

Commit before you reveal. Always.

RISK DECK

STEP 2 · PRIVATE

PREDICTION TRACKER

TRACK

MY READ

beat 1, before anyone shares

LIKELIHOOD

1

2

3

4

5

IMPACT

T1

T2

T3

T4

T5

I PREDICT ____ WILL SAY

beat 1, blind guess of a cross-Lens player

LIKELIHOOD

1

2

3

4

5

IMPACT

T1

T2

T3

T4

T5

AFTER WE SHARE

beat 2, re-commit together

LIKELIHOOD

1

2

3

4

5

IMPACT

T1

T2

T3

T4

T5

Fill the top two blind. Fill the last one after we talk.

RISK DECK

BOARDROOM · COST

WHAT DOES IT COST?

BOARDROOM

"Give me the number. What does this cost us, and is it a one-time hit or does it bleed?"

ASKED BY THE CFO

ANSWER IN PLAIN LANGUAGE

60 SEC

TECH → BUSINESS

IC probe: If they say "it depends," make them give a range, not a dodge.

RISK DECK

BOARDROOM · RECOVERY

WHEN ARE WE BACK?

BOARDROOM

"It is Friday at 17:00 and we are down. When are we back, and what does every hour offline cost?"

ASKED BY THE COO

ANSWER IN PLAIN LANGUAGE

60 SEC

TECH → BUSINESS

IC probe: Push for who cannot work and what stops selling.

RISK DECK

BOARDROOM · REGULATORY

WERE WE NEGLIGENCE?

BOARDROOM

"A regulator asks whether we were negligent. Answer in plain English, no frameworks."

ASKED BY THE GENERAL COUNSEL

ANSWER IN PLAIN LANGUAGE

90 SEC

TECH → BUSINESS

IC probe: If they name a standard, make them say what it means in one sentence.

RISK DECK

BOARDROOM · NOTIFICATION

WHO DO WE TELL?

BOARDROOM

"Do we have to tell anyone, who, and by when? Yes or no first, then why."

ASKED BY THE DPO

ANSWER IN PLAIN LANGUAGE

60 SEC

TECH → BUSINESS

IC probe: Ask what starts the clock.

RISK DECK

BOARDROOM · REPUTATION

WHAT DO WE TELL THEM?

BOARDROOM

"Our largest customer is about to read this in the press. What do we tell them, in two sentences?"

ASKED BY THE CEO

ANSWER IN PLAIN LANGUAGE

60 SEC

TECH → BUSINESS

IC probe: Ban jargon. If they hedge, ask "would that actually reassure you?"

RISK DECK

20mm ruler. Off? Reprint at 100% / Actual Size.

So, tell me...

what's the worst thing
that could happen?



RISK DECK

· CLUE ·

So, tell me...

what's the worst thing
that could happen?



RISK DECK

· CLUE ·

So, tell me...

what's the worst thing
that could happen?



RISK DECK

· CLUE ·

So, tell me...

what's the worst thing
that could happen?



RISK DECK

· BOARDROOM ·

So, tell me...

what's the worst thing
that could happen?



RISK DECK

· BOARDROOM ·

So, tell me...

what's the worst thing
that could happen?



RISK DECK

· CLUE ·

So, tell me...

what's the worst thing
that could happen?



RISK DECK

· BOARDROOM ·

So, tell me...

what's the worst thing
that could happen?



RISK DECK

· BOARDROOM ·

So, tell me...

what's the worst thing
that could happen?



RISK DECK

· BOARDROOM ·

BOARDROOM · FUNDING

WHAT DOES IT BUY DOWN?

BOARDROOM

"You want budget for the control you just played. What risk does it buy down, in money?"

ASKED BY THE CFO

ANSWER IN PLAIN LANGUAGE

90 SEC

TECH → BUSINESS

IC probe: Make them tie it to a Target value on the table.

RISK DECK

BOARDROOM · COMPARISON

WHY ARE WE DIFFERENT?

BOARDROOM

"Competitor X had this exact breach last quarter. Why are we different, or are we not?"

ASKED BY A BOARD MEMBER

ANSWER IN PLAIN LANGUAGE

60 SEC

TECH → BUSINESS

IC probe: If "we are fine," demand the one reason.

RISK DECK

BOARDROOM · DECISION

ACCEPT, MITIGATE, TRANSFER?

BOARDROOM

"I decide in this meeting. One word: accept, mitigate, or transfer. Then defend it in two sentences."

ASKED BY THE CHAIR

ANSWER IN PLAIN LANGUAGE

60 SEC

TECH → BUSINESS

IC probe: Hold them to the one word before the defence.

RISK DECK

BOARDROOM · COMMIT

WOULD IT HAVE STOPPED THIS?

BOARDROOM

"You just funded that control. Would it actually have stopped this attack? Yes or no, then why."

THE BOARD ASKS THE BUSINESS VOICE

ANSWER IN PLAIN LANGUAGE

60 SEC

BUSINESS → TECH

IC probe: The technical camp grades the answer, it does not correct it.

RISK DECK

BOARDROOM · EXPLAIN BACK

SAY THAT IN PLAIN ENGLISH

BOARDROOM

"The team keeps saying lateral movement, persistence, C2. Explain one back to me in one plain sentence."

THE BOARD ASKS THE BUSINESS VOICE

ANSWER IN PLAIN LANGUAGE

45 SEC

BUSINESS → TECH

IC probe: The technical camp gives only a thumbs up or down.

RISK DECK

BOARDROOM · PRIORITIZE

WHICH IS THE BIGGER RISK?

BOARDROOM

"Two findings on the table. Which is the bigger business risk, and why? Pick one."

THE BOARD ASKS THE BUSINESS VOICE

ANSWER IN PLAIN LANGUAGE

60 SEC

BUSINESS → TECH

IC probe: Ask what would change your mind.

RISK DECK

BOARDROOM · SCOPE

HOW MANY, REALISTICALLY?

BOARDROOM

"How many customers or records, realistically? Give me a range, never "it depends.""

ASKED BY THE BOARD

ANSWER IN PLAIN LANGUAGE

60 SEC

EITHER CAMP

IC probe: Anchor the range to the Target's importance value.

RISK DECK

CONTROL · PREVENT

MULTI-FACTOR AUTHENTICATION

CONTROL

Stolen or guessed credentials stop being enough on their own. Lands against any step whose way in was a password.

NIST 800-53 IA-2(1) · ISO 27001 A.8.5 · CIS 6.5

TABLEAU · ONE SHOT

Face up on the table all session — play it from the tableau, never from a hand. Once it lands, turn this card sideways: used for the rest of the session.

Ask which account. "Everywhere" is not an answer.

RISK DECK

CONTROL · DETECT

ENDPOINT DETECTION &...

CONTROL

Someone sees the Actor running code on a host, early enough to act. Lands against an execution or persistence step.

NIST 800-53 SI-4 · ISO 27001 A.8.7 · CIS 10.7

TABLEAU · ONE SHOT

Face up on the table all session — play it from the tableau, never from a hand. Once it lands, turn this card sideways: used for the rest of the session.

Who is watching it at 02:00? If nobody, say so.

RISK DECK

So, tell me... what's the worst thing that could happen?  RISK DECK · BOARDROOM ·	So, tell me... what's the worst thing that could happen?  RISK DECK · BOARDROOM ·	So, tell me... what's the worst thing that could happen?  RISK DECK · BOARDROOM ·
So, tell me... what's the worst thing that could happen?  RISK DECK · BOARDROOM ·	So, tell me... what's the worst thing that could happen?  RISK DECK · BOARDROOM ·	So, tell me... what's the worst thing that could happen?  RISK DECK · BOARDROOM ·
So, tell me... what's the worst thing that could happen?  RISK DECK · CONTROL ·	So, tell me... what's the worst thing that could happen?  RISK DECK · CONTROL ·	So, tell me... what's the worst thing that could happen?  RISK DECK · BOARDROOM ·

CONTROL · PREVENT

NETWORK SEGMENTATION

The Actor lands in one zone instead of the estate. Lands against a pivot or lateral-movement step.

NIST 800-53 SC-7 · ISO 27001 A.8.22 · CIS 12.2

TABLEAU · ONE SHOT

Face up on the table all session — play it from the tableau, never from a hand. Once it lands, turn this card sideways: used for the rest of the session.

Name the two zones and what still crosses between them.

RISK DECK

CONTROL · RESPOND

IMMUTABLE OFFLINE BACKUPS

Recovery stops depending on the Actor's goodwill. Lands against a destruction, encryption or tamper step.

NIST 800-53 CP-9 · ISO 27001 A.8.13 · CIS 11.4

TABLEAU · ONE SHOT

Face up on the table all session — play it from the tableau, never from a hand. Once it lands, turn this card sideways: used for the rest of the session.

When was the last restore actually tested end to end?

RISK DECK

CONTROL · PREVENT

SECURITY AWARENESS...

A person spots the approach and reports it instead of clicking. Lands against a phishing or social-engineering step.

NIST 800-53 AT-2 · ISO 27001 A.6.3 · CIS 14.1

TABLEAU · ONE SHOT

Face up on the table all session — play it from the tableau, never from a hand. Once it lands, turn this card sideways: used for the rest of the session.

Reporting rate beats click rate. Which one do you measure?

RISK DECK

CONTROL · RESPOND

TESTED INCIDENT RESPONSE PLAN

The first hour is rehearsed, not improvised, so the chain gets cut sooner. Lands against any step after initial access.

NIST 800-53 IR-8 · ISO 27001 A.5.24 · CIS 17.4

TABLEAU · ONE SHOT

Face up on the table all session — play it from the tableau, never from a hand. Once it lands, turn this card sideways: used for the rest of the session.

A plan nobody has exercised is a document, not a control.

RISK DECK

CONTROL · PREVENT

ENCRYPTION AT REST

Reaching the storage is no longer the same as reading it. Lands against a data-access or exfiltration step.

NIST 800-53 SC-28 · ISO 27001 A.8.24 · CIS 3.11

TABLEAU · ONE SHOT

Face up on the table all session — play it from the tableau, never from a hand. Once it lands, turn this card sideways: used for the rest of the session.

Where do the keys live? If beside the data, it does not land.

RISK DECK

CONTROL · GOVERN

THIRD-PARTY RISK ASSESSMENT

The supplier path gets looked at before it is used against you. Lands against a supply-chain or vendor-access step.

NIST 800-53 SR-6 · ISO 27001 A.5.19 · CIS 15.2

TABLEAU · ONE SHOT

Face up on the table all session — play it from the tableau, never from a hand. Once it lands, turn this card sideways: used for the rest of the session.

Which vendor reaches your production right now?

RISK DECK

CONSEQUENCE · SHIFT PROMPT

CONFIDENTIALITY

Secrets get out. Data that should have stayed private is now somewhere else.

ASK OUT LOUD

Is regulated or personal data involved?

ONE BUMP PER ROW

A yes shifts that row's Impact up one tier. One bump per row, no stacking — a second yes changes the argument, not the number.

'Probably not' is a no. Make them commit.

RISK DECK

CONSEQUENCE · SHIFT PROMPT

INTEGRITY

Numbers or records are quietly wrong, and nothing announces it.

ASK OUT LOUD

Would the business act on the corrupted data before anyone noticed?

ONE BUMP PER ROW

A yes shifts that row's Impact up one tier. One bump per row, no stacking — a second yes changes the argument, not the number.

Ask who would have caught it, and when.

RISK DECK

CONSEQUENCE · SHIFT PROMPT

AVAILABILITY

The thing is simply not there when the business reaches for it.

ASK OUT LOUD

Is this revenue- or safety-critical? If yes, read the band as cost per hour down, times duration.

ONE BUMP PER ROW

A yes shifts that row's Impact up one tier. One bump per row, no stacking — a second yes changes the argument, not the number.

Get the hourly number before the duration.

RISK DECK

So, tell me...

what's the worst thing
that could happen?



RISK DECK

· CONTROL ·

So, tell me...

what's the worst thing
that could happen?



RISK DECK

· CONTROL ·

So, tell me...

what's the worst thing
that could happen?



RISK DECK

· CONTROL ·

So, tell me...

what's the worst thing
that could happen?



RISK DECK

· CONTROL ·

So, tell me...

what's the worst thing
that could happen?



RISK DECK

· CONTROL ·

So, tell me...

what's the worst thing
that could happen?



RISK DECK

· CONTROL ·

So, tell me...

what's the worst thing
that could happen?



RISK DECK

· CONSEQUENCE ·

So, tell me...

what's the worst thing
that could happen?



RISK DECK

· CONSEQUENCE ·

So, tell me...

what's the worst thing
that could happen?



RISK DECK

· CONSEQUENCE ·

CONSEQUENCE · HUMAN IMPACT

HUMAN IMPACT

CONSEQUENCE

Some damage never shows up on a balance sheet. This prompt puts it on the table anyway.

ASK OUT LOUD

Does this harm a person, not just a balance sheet?

ONE BUMP PER ROW

A yes shifts that row's Impact up one tier. One bump per row, no stacking — a second yes changes the argument, not the number.

if the answer is yes and nobody shifts, ask them to justify it out loud.

RISK DECK

COLD START · ACTOR

NATION STATE

ACTOR

A government-backed group running espionage or sabotage. Patient, funded, and already finished its reconnaissance.

5

SUGGESTED STRENGTH

1–5, suggested — the group may adjust it

OPTIONAL COLD START

Setup only, and only if nobody brought a real incident. Flip one Actor and one Target blind, face down. The pack is done after setup.

The hardest opener. Swap it out if the table stalls.

RISK DECK

COLD START · ACTOR

ORGANIZED CRIME

ACTOR

In it for money, so they automate and run the same weakness across everyone at once.

4

SUGGESTED STRENGTH

1–5, suggested — the group may adjust it

OPTIONAL COLD START

Setup only, and only if nobody brought a real incident. Flip one Actor and one Target blind, face down. The pack is done after setup.

Ask what makes you worth the automation.

RISK DECK

COLD START · ACTOR

INSIDER

ACTOR

The access is already inside the perimeter, and it was granted on purpose.

3

SUGGESTED STRENGTH

1–5, suggested — the group may adjust it

OPTIONAL COLD START

Setup only, and only if nobody brought a real incident. Flip one Actor and one Target blind, face down. The pack is done after setup.

Malicious or careless? Decide before you estimate.

RISK DECK

COLD START · ACTOR

HACKTIVIST

ACTOR

Driven by a cause and a deadline. Moderate capability, motivation spikes around a trigger.

3

SUGGESTED STRENGTH

1–5, suggested — the group may adjust it

OPTIONAL COLD START

Setup only, and only if nobody brought a real incident. Flip one Actor and one Target blind, face down. The pack is done after setup.

Name the trigger. No trigger, lower the Strength.

RISK DECK

COLD START · ACTOR

OPPORTUNIST

ACTOR

Public tooling and known exploits. Stopped cold by hygiene, devastating wherever hygiene lapsed.

2

SUGGESTED STRENGTH

1–5, suggested — the group may adjust it

OPTIONAL COLD START

Setup only, and only if nobody brought a real incident. Flip one Actor and one Target blind, face down. The pack is done after setup.

The most realistic opener for most orgs.

RISK DECK

COLD START · TARGET

CUSTOMER PRIVATE DATA

TARGET

Personal data your customers trusted you with. Losing it starts clocks you do not control.

8

SUGGESTED IMPORTANCE

1–10, suggested — the group may adjust it

OPTIONAL COLD START

Setup only, and only if nobody brought a real incident. Flip one Actor and one Target blind, face down. The pack is done after setup.

Regulated? Then the Confidentiality prompt will fire.

RISK DECK

COLD START · TARGET

CORE PRODUCTION SYSTEM

TARGET

The system the business runs on. Every hour down is revenue not earned.

9

SUGGESTED IMPORTANCE

1–10, suggested — the group may adjust it

OPTIONAL COLD START

Setup only, and only if nobody brought a real incident. Flip one Actor and one Target blind, face down. The pack is done after setup.

Get the cost-per-hour before anyone estimates.

RISK DECK

COLD START · TARGET

FINANCIAL RECORDS

TARGET

The numbers the business makes decisions on. Quiet alteration is worse than loud theft.

7

SUGGESTED IMPORTANCE

1–10, suggested — the group may adjust it

OPTIONAL COLD START

Setup only, and only if nobody brought a real incident. Flip one Actor and one Target blind, face down. The pack is done after setup.

Who would notice, and how late?

RISK DECK

So, tell me...

what's the worst thing
that could happen?



RISK DECK

· ACTOR ·

So, tell me...

what's the worst thing
that could happen?



RISK DECK

· ACTOR ·

So, tell me...

what's the worst thing
that could happen?



RISK DECK

· CONSEQUENCE ·

So, tell me...

what's the worst thing
that could happen?



RISK DECK

· ACTOR ·

So, tell me...

what's the worst thing
that could happen?



RISK DECK

· ACTOR ·

So, tell me...

what's the worst thing
that could happen?



RISK DECK

· ACTOR ·

So, tell me...

what's the worst thing
that could happen?



RISK DECK

· TARGET ·

So, tell me...

what's the worst thing
that could happen?



RISK DECK

· TARGET ·

So, tell me...

what's the worst thing
that could happen?



RISK DECK

· TARGET ·

COLD START · TARGET SOURCE CODE & IP TARGET Years of work, and often the thing that makes the product defensible at all. 6 SUGGESTED IMPORTANCE 1–10, suggested — the group may adjust it OPTIONAL COLD START Setup only, and only if nobody brought a real incident. Flip one Actor and one Target blind, face down. The pack is done after setup. Any secrets committed in there? Raise it. RISK DECK	COLD START · TARGET BACKUPS TARGET The line between an incident and a catastrophe. Hit these and recovery becomes hope. 8 SUGGESTED IMPORTANCE 1–10, suggested — the group may adjust it OPTIONAL COLD START Setup only, and only if nobody brought a real incident. Flip one Actor and one Target blind, face down. The pack is done after setup. Online backups are production. Say it out loud. RISK DECK	

	So, tell me... what's the worst thing that could happen?  RISK DECK • TARGET •	So, tell me... what's the worst thing that could happen?  RISK DECK • TARGET •