

CYBER RISK

Baseline Assessment

Illustrative sample report

PREPARED FOR

Harborline Fabrication, Inc.

Illustrative manufacturing client · September 2026

SAMPLE NOTICE

This document demonstrates Refuge's intended reporting format. The organization, environment, data, findings, and recommendations are fictional and do not represent completed customer work.

Executive perspective

WHAT LEADERSHIP NEEDS TO KNOW

The short version

The illustrative environment has a workable foundation, but several gaps could amplify the impact of an account compromise, ransomware event, or prolonged outage. The strongest early moves are to protect privileged access and prove that critical data and systems can be restored.

13

OBSERVATIONS

Items noted across the authorized scope.

04

PRIORITY ACTIONS

Actions recommended in the next 30 days.

90

DAY ROADMAP

A practical sequence to reduce exposure.

PRIMARY CONCERN

Recovery capability is not verified. Successful backup jobs do not prove that critical data and systems can be restored within an acceptable time.

IMMEDIATE PRIORITY

Require strong multifactor authentication for privileged accounts and review who retains elevated access.

ILLUSTRATIVE OVERALL POSTURE

ELEVATED RISK

The sample score reflects a business-impact view of the fictional findings—not a certification, maturity score, or compliance rating.

Risk at a glance

ILLUSTRATIVE OBSERVATIONS ACROSS THE ASSESSMENT SCOPE

Where attention is concentrated

The chart below groups illustrative observations by the likely business impact and urgency of corrective action. It is intended to help leadership see priorities at a glance.

RELATIVE PRIORITY BY REVIEW AREA • SAMPLE DATA



Illustrative finding register

ID	RISK	FINDING	OWNER	TARGET
F1	HIGH	Privileged MFA is inconsistent	IT Lead	14 days
F2	HIGH	Recovery testing remains unverified	Operations	30 days
F3	MODERATE	Endpoint safeguards are unmanaged	IT Lead	60 days
F4	MODERATE	Third-party apps are unreviewed	IT Lead	30 days
F5	MODERATE	Vendor access lacks review ownership	Operations	60 days

Priority finding · F1

PRIVILEGED ACCESS LACKS CONSISTENT MULTIFACTOR AUTHENTICATION

HIGH RISK

Control of privileged access

Illustrative observation: selected administrative accounts were not consistently protected with multifactor authentication. In this fictional environment, those accounts can change security settings, access email and files, and reset other user passwords.

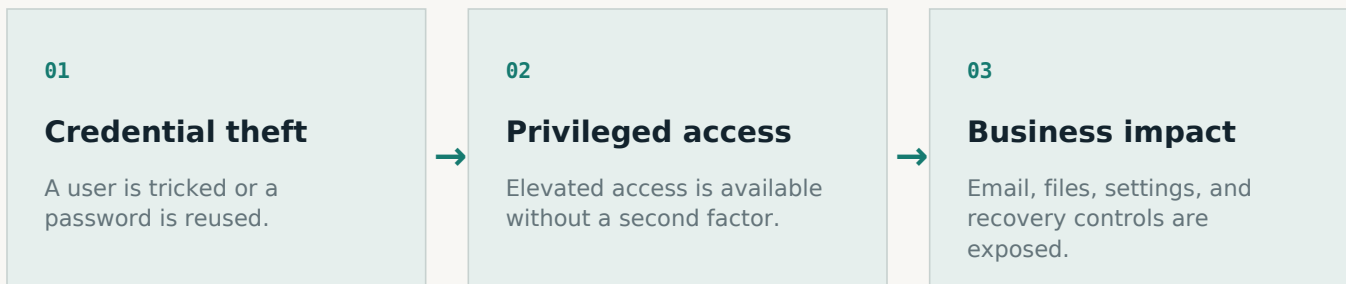
WHY IT MATTERS

A stolen credential or session could give an attacker broad access, making a contained account compromise much harder to stop.

RECOMMENDED ACTION

Require strong multifactor authentication for every privileged account, reduce standing administrative access, and review elevated roles on a defined schedule.

ILLUSTRATIVE EXPOSURE PATH



VALIDATION EVIDENCE

Administrative-account inventory; confirmation of multifactor authentication enforcement; reduced role assignments; assigned owner and recurring access-review date.

Priority finding · F2

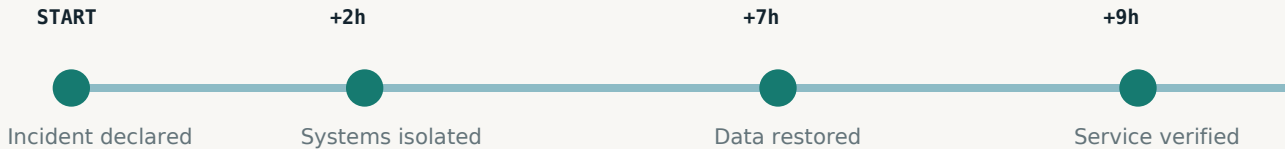
RECOVERY CAPABILITY HAS NOT BEEN DEMONSTRATED

HIGH RISK

Backups are present. Recovery is unverified

Illustrative observation: backup software reported successful jobs for critical file and application data, but the fictional organization could not provide evidence of a recent restoration test, a documented recovery target, or a protected copy isolated from administrative compromise.

ILLUSTRATIVE RECOVERY TEST TIMELINE



WHAT THIS TEST PROVES

Whether the selected data can be recovered, how long it takes, what dependencies are missing, and who needs to act.

RECOMMENDED NEXT ACTION

Perform a documented restoration test using representative data and one business-critical system. Capture recovery time, data-loss window, issues, and corrective actions.

LEADERSHIP QUESTION

How long can this business function be unavailable before the impact becomes unacceptable?

90-day roadmap

A PRACTICAL SEQUENCE TO REDUCE EXPOSURE

Focus on the work that changes the risk picture

This is an illustrative roadmap. Ownership, timing, and sequencing are tailored to the

0–14 DAYS

Protect access

- Enforce MFA for privileged accounts
- Remove unneeded elevated access
- Confirm incident contact list

15–45 DAYS

Prove recovery

- Run a representative restoration test
- Set recovery objectives
- Protect an offline or immutable copy

46–90 DAYS

Standardize & sustain

- Establish endpoint baseline
- Review third-party access
- Track progress with leadership

EXPECTED RESULT

A clearer view of who owns the work, which actions have been completed, and where leadership decisions are still needed.

What the assessment delivers

USEFUL CLARITY FOR THE NEXT DECISION

LEADERSHIP-READY SUMMARY

A concise explanation of material risks, business consequences, and decisions that need an owner.

PRIORITIZED FINDINGS

A documented record of significant observations with clear recommendations and target timeframes.

PRACTICAL ROADMAP

A sequence of work that matches the organization's actual risk, resources, and operating needs.

LEADERSHIP DISCUSSION

A walk-through of the results so the next actions are understood, owned, and realistic.

A NOTE ABOUT THE SAMPLE

This fictional report illustrates how Refuge connects technical observations to business decisions. A real engagement is scoped in advance, based on authorized access, and designed around your organization's actual risks and resources.

REFUGE RISK & RESILIENCE

Independent cybersecurity guidance for small and midsized businesses.