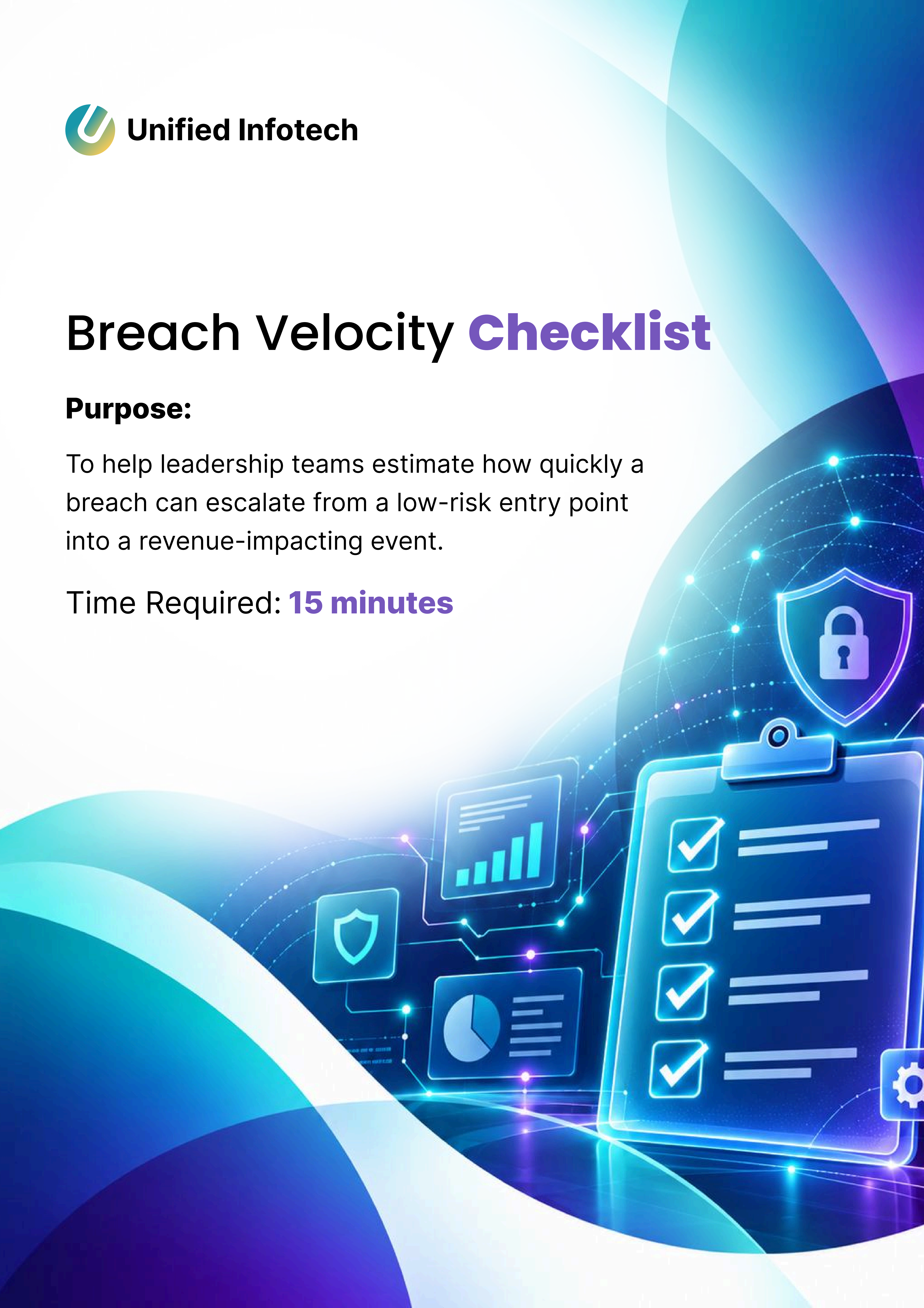


Breach Velocity Checklist

Purpose:

To help leadership teams estimate how quickly a breach can escalate from a low-risk entry point into a revenue-impacting event.

Time Required: **15 minutes**



Question	Yes	No	Don't Know
SECTION A: Permission Is the Perimeter (Access and Integrations)			
Do we list all third-party apps with Read/Write access to customer data?	☐	☐	☐
Have we revoked/reviewed tokens in the last 30 days?	☐	☐	☐
Can we disable third-party API permissions within 15 minutes?	☐	☐	☐
Is least privilege access our default?	☐	☐	☐
Risk Flag: If any answer is "Don't Know," escalation can be fast.			
Question	Yes	No	Don't Know
SECTION B. Zombie Assets (The Forgotten Entry Points)			
Can we list all live URLs, subdomains, microsites, and staging sites within 48 hours?	☐	☐	☐
Are staging and sandbox environments access-restricted and unindexed?	☐	☐	☐
Have we deleted at least 20% of unused URLs in the last quarter?	☐	☐	☐
Do we patch and monitor non-primary web properties with the same urgency as the main site?	☐	☐	☐
Risk Flag: Unknown assets equal unknown entry points.			

Question	Yes	No	Don't Know
SECTION C. Identity and Executive Impersonation (Human API Risk)			
Do we have a written protocol for “urgent CEO requests”?	☐	☐	☐
Do we require a non-voice verification step for high-risk approvals?	☐	☐	☐
Have we trained executive-facing teams to treat voice and messaging as spoofable?	☐	☐	☐
Risk Flag: If identity checks rely on recognition alone, escalation becomes immediate.			
Question	Yes	No	Don't Know
SECTION D. Recovery Over Prevention (Revenue Continuity)			
If our primary site went down today, do we know our Recovery Time Objective in minutes or hours?	☐	☐	☐
Do we have a fallback plan if our most critical plugin/API goes dark?	☐	☐	☐
When did we last run a full executive tabletop simulation of a total outage?	☐	☐	☐
Risk Flag: Slow recovery turns incidents into crises.			

Question	Yes	No	Don't Know
SECTION E. Detection and Speed (The Only Metric That Matters)			
Do we know how long it takes us to detect abnormal access to customer data?	☐	☐	☐
Do we know how long it takes us to revoke access and contain lateral movement?	☐	☐	☐
Do we monitor for token misuse, unusual admin actions, and abnormal API patterns?	☐	☐	☐

Risk Flag: If you can't answer these with a number, you're flying blind.

SCORING for "No/Don't Know"

0-4	Controlled velocity
5-8	Elevated velocity
9 +	Critical velocity risk

If your team has 5+ "No/Don't Know", you don't have a "security gap." You have a breach velocity problem. Run a controlled escalation simulation NOW!