BREACHRX

REGULATORY CONCURRENCY:

Why cyber incident reporting is no longer human-scalable

The New Reality

100+

Concurrent obligations

A single incident can trigger 100+ disclosure deadlines

The scaling failure

Manual coordination via email and spreadsheets is no longer defensible

300+

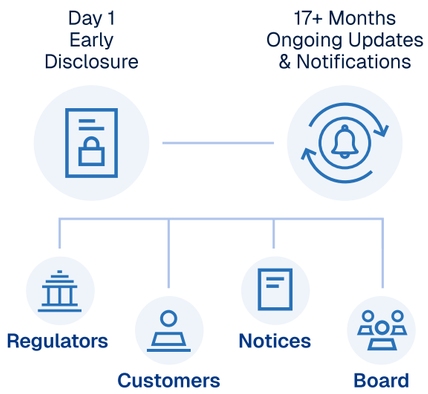
Cascading obligations

Multi-tenant compromises can drive 300+ obligations as secondary incidents multiply

The 5 Archetypes of Regulatory Concurrency

Vertical concurrency

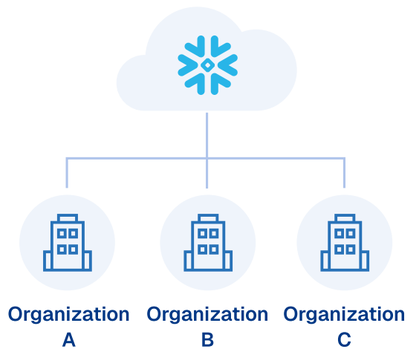
(Time-driven)



Disclosure clocks start at different times and run at different speeds

Horizontal concurrency

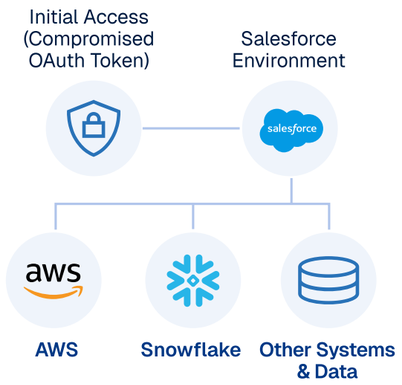
(Org-driven)



One root cause creates many independent reporting systems

Cascading concurrency

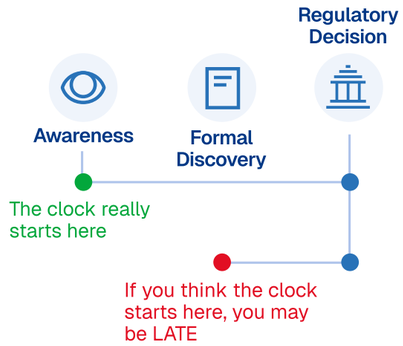
(System-driven)



Downstream access expands scope to new environments during investigation

Definition-driven concurrency

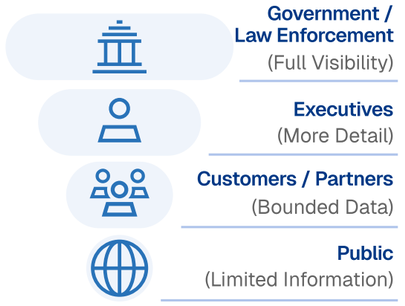
(Trigger-driven)



The gap between “awareness” and “formal discovery” can make you late

Constraint-driven concurrency

(Visibility-driven)



Legal, regulatory, or national security limits create narrative asymmetry

⚠ Impact

Sustained pressure for months	Shared incidents, independent reporting	Incidents generate more incidents	Timing ambiguity is dangerous	The problem of restricted disclosure

More deadlines. More incidents. Less time. Tame the chaos.

This analysis is derived from the BreachRx Regulatory Concurrency Report.

Five major incidents analyzed: • Change healthcare • Snowflake • Salesforce • 700Credit • Salt Typhoon

DOWNLOAD NOW →