THE SYSTEM CFO SERIES

HINDOL DATTA

FREE ASSESSMENT

PILLAR 5: GOVERNANCE & GLOBAL STRUCTURE | TOOLKIT #36 OF 37

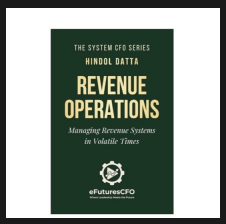
THE DATA BREACH FINANCIAL PREPAREDNESS DIAGNOSTIC

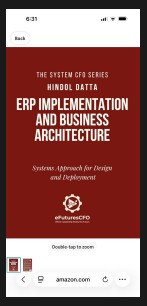
Quantifying the Cost Before the Breach — Not After

20-Question Diagnostic | 5-Page Assessment

Score Your Organization 1-5 Across Four Dimensions

Identify Gaps and Build Your Action Plan





EfuturesCFO.com

Where Leadership Meets the Future

QUESTIONS 1-5

Section A: Financial Exposure Quantification

Do You Know What a Data Breach Would Cost You — In Dollars, Not Just Headlines?

> *The average cost of a data breach exceeds $4.5 million, but the financial impact varies enormously based on the type of data compromised, the speed of detection, the regulatory environment, and the organization's preparedness. The System CFO quantifies potential breach costs before an incident occurs — including direct costs, regulatory fines, litigation exposure, business disruption, and reputation damage — so that insurance, reserves, and response plans are calibrated to actual risk.*

A. FINANCIAL EXPOSURE QUANTIFICATION

1	The organization has modeled the financial impact of a data breach — including notification costs, forensic investigation, legal fees, regulatory fines, credit monitoring, business	1 Non-Ex	2 Ad Hoc	3 Dev	4 Estab	5 Best
2	Different breach scenarios have been costed — the financial impact varies by breach type (customer PII, payment data, employee records, trade secrets), and multiple scenarios have	1 Non-Ex	2 Ad Hoc	3 Dev	4 Estab	5 Best
3	Cyber insurance coverage is adequate and current — the organization has evaluated whether its cyber insurance policy covers the estimated breach costs, with limits, deductibles,	1 Non-Ex	2 Ad Hoc	3 Dev	4 Estab	5 Best
4	Regulatory fine exposure has been assessed — for organizations subject to GDPR, CCPA, HIPAA, or other data protection regulations, the potential fine amounts for different	1 Non-Ex	2 Ad Hoc	3 Dev	4 Estab	5 Best
5	The business disruption cost of a breach is estimated — beyond direct breach costs, the organization has modeled the impact of system downtime, operational disruption, and delayed	1 Non-Ex	2 Ad Hoc	3 Dev	4 Estab	5 Best

SECTION A SCORE: Total: _____ / 25 Average: _____ / 5

QUESTIONS 6-10

Section B: Financial Controls for Breach Response

If a Breach Happened Tonight, Could Finance Execute Its Part of the Response Plan?

The finance function has specific responsibilities during a data breach: activating insurance, authorizing emergency expenditures, engaging forensic and legal vendors, managing disclosure obligations, and tracking costs for potential recovery. The System CFO ensures that these financial response capabilities are documented, tested, and ready for activation without delay when an incident occurs.

B. FINANCIAL CONTROLS FOR BREACH RESPONSE

6	Emergency expenditure authority is pre-approved — the CFO has authority to authorize breach response spending up to defined limits without requiring board approval, enabling rapid	1 Non-Ex	2 Ad Hoc	3 Dev	4 Estab	5 Best
7	Cyber insurance claim procedures are documented — the finance team knows the notification requirements, coverage triggers, documentation needs, and adjuster contacts for the cyber	1 Non-Ex	2 Ad Hoc	3 Dev	4 Estab	5 Best
8	Pre-negotiated vendor agreements exist for breach response — retainer arrangements with forensic investigators, breach notification vendors, credit monitoring providers, and	1 Non-Ex	2 Ad Hoc	3 Dev	4 Estab	5 Best
9	Breach cost tracking procedures are ready — a cost center, project code, or tracking mechanism is defined so that all breach-related expenditures can be captured accurately from	1 Non-Ex	2 Ad Hoc	3 Dev	4 Estab	5 Best
10	The finance team participates in the incident response plan — the CFO or designated finance representative is included in the incident response team with defined responsibilities for	1 Non-Ex	2 Ad Hoc	3 Dev	4 Estab	5 Best

SECTION B SCORE: Total: _____ / 25 Average: _____ / 5

QUESTIONS 11-15

Section C: Financial Reporting and Disclosure Obligations

Can You Meet Your Disclosure Obligations — Accurately and On Time?

Data breaches create financial reporting obligations. Public companies must evaluate whether a breach constitutes a material event requiring SEC disclosure. All organizations must assess whether a loss contingency reserve is required under ASC 450. The System CFO ensures that the finance team is prepared to meet these reporting obligations with the accuracy, speed, and judgment that regulators and auditors expect.

C. FINANCIAL REPORTING AND DISCLOSURE OBLIGATIONS

11	The organization understands its disclosure obligations — for public companies, SEC rules on cyber incident disclosure (including the 4-day Form 8-K requirement) are understood and	1 Non-Ex	2 Ad Hoc	3 Dev	4 Estab	5 Best
12	Loss contingency assessment procedures exist — the finance team has a defined process for evaluating whether a breach requires a reserve under ASC 450, including criteria for	1 Non-Ex	2 Ad Hoc	3 Dev	4 Estab	5 Best
13	The impact on financial statements has been considered — potential impacts on revenue (customer loss), expenses (remediation costs), and balance sheet (contingent	1 Non-Ex	2 Ad Hoc	3 Dev	4 Estab	5 Best
14	Communication with external auditors is planned — the procedure for notifying external auditors of a data breach and providing the information they need for their assessment is	1 Non-Ex	2 Ad Hoc	3 Dev	4 Estab	5 Best
15	Investor and stakeholder communication includes financial impact — the organization is prepared to communicate the estimated financial impact of a breach to investors, lenders,	1 Non-Ex	2 Ad Hoc	3 Dev	4 Estab	5 Best

SECTION C SCORE: Total: _____ / 25 Average: _____ / 5

QUESTIONS 16-20

Section D: Prevention Investment and Risk Governance

Are You Investing Enough in Prevention — and Does the Board Have Visibility?

> *The most cost-effective approach to breach costs is prevention. Every dollar invested in cybersecurity controls, employee training, and vendor risk management reduces the probability and severity of a breach. The System CFO evaluates cybersecurity spending as a risk reduction investment — not just an IT cost — and ensures the board understands the relationship between security investment and financial risk exposure.*

D. PREVENTION INVESTMENT AND RISK GOVERNANCE

16	Cybersecurity spending is evaluated as risk reduction — the organization frames security investment in terms of the financial risk it mitigates, enabling informed cost-benefit	1 Non-Ex	2 Ad Hoc	3 Dev	4 Estab	5 Best
17	The board receives regular reporting on cyber risk — including the organization's risk posture, recent threat landscape changes, security investment levels, insurance coverage, and	1 Non-Ex	2 Ad Hoc	3 Dev	4 Estab	5 Best
18	Tabletop exercises include financial scenarios — the organization has conducted breach simulation exercises that test the finance team's response capabilities, not just the	1 Non-Ex	2 Ad Hoc	3 Dev	4 Estab	5 Best
19	The organization tracks cybersecurity maturity over time — using a framework like NIST CSF, CIS Controls, or ISO 27001 to measure and report on the trajectory of the security program	1 Non-Ex	2 Ad Hoc	3 Dev	4 Estab	5 Best
20	Post-breach improvement processes exist — if a breach or near-miss occurs, the organization conducts a thorough review that includes financial impact assessment, insurance adequacy	1 Non-Ex	2 Ad Hoc	3 Dev	4 Estab	5 Best

SECTION D SCORE: Total: _____ / 25 Average: _____ / 5

OVERALL ASSESSMENT SCORE

Section A: ___ / 25 Section B: ___ / 25 Section C: ___ / 25 Section D: ___ / 25 TOTAL: ___ / 100 AVG: ___ / 5

GAP TO GOAL

Gap-to-Goal Action Plan

Bridging the Gap — Data Breach Financial Preparedness Diagnostic

Transfer your five lowest-scoring questions. For each gap, define the target state, specific actions, owner, timeline, and success metric. Focus on highest-impact gaps first.

GAP #	Q REF	CURRENT	TARGET	SPECIFIC ACTION TO CLOSE GAP	OWNER	DEADLINE	METRIC
1	Q___	___/5	___/5				
2	Q___	___/5	___/5				
3	Q___	___/5	___/5				
4	Q___	___/5	___/5				
5	Q___	___/5	___/5				

ASSESSMENT SUMMARY

Completed by: _____ Date: _____

Overall average score: _____ / 5 Items scored 1-2 (critical): _____

Items scored 3 (developing): _____ Items scored 4-5 (strong): _____

Top strength: _____

Most critical gap: _____

One action this week: _____

READY TO GO DEEPER?

This free assessment identified your gaps. The Premium System CFO Toolkits provide the frameworks, templates, and action plans to close them. Visit EfuturesCFO.com

READY TO GO DEEPER?

This Assessment Identified the Gaps. The Premium Toolkit Closes Them.

PREMIUM: The AI Governance Readiness Scorecard (12 Pages)

The full premium toolkit includes the comprehensive AI and technology governance framework with risk classification, data protection assessment, vendor evaluation tools, incident response protocols, and the complete governance charter template applicable to both AI and cybersecurity risk management.

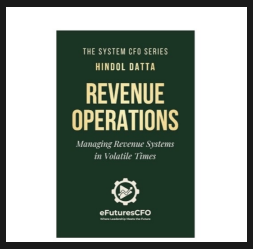
Plus: Access the Super Exclusive 46-Page System CFO Organizational Finance Assessment Kit

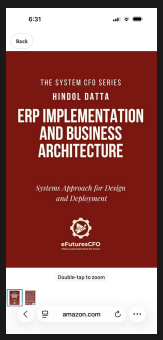
ABOUT THE AUTHOR

Hindol Datta

25+ years as CFO and VP Finance | $150M+ in M&A | CPA, CMA, CIA, PMP, CPIM

Author of The System CFO Series | MS Analytics, Georgia Tech





EfuturesCFO.com

LinkedIn: Hindol Datta | YouTube: @efuturescfo

Where Leadership Meets the Future