SecureBank™

A Systemic Cyber Risk Modeling Framework for Financially Regulated Infrastructures

Quantifying financial, operational, and regulatory exposure in cyber-driven systemic failures

Author: Paulo Fernandes Biao

Version: v1.0 (Core Whitepaper + Appendices)

Date: January 6, 2026

Note: This document presents SecureBank as a conceptual decision-grade framework designed for financially regulated environments.

Executive Brief

Purpose

Enable executive leadership to **quantify systemic cyber risk**, compare strategic options, and make **defensible financial and regulatory decisions** before cyber incidents materialize.

The Executive Problem

Cybersecurity decisions in financially regulated institutions remain driven by compliance posture, control maturity, and qualitative risk ratings. These instruments describe *what controls exist*, but they do not answer the question that defines executive accountability:

> **How much money will the institution lose — and how fast — under a realistic cyber failure scenario?**

As financial architectures become increasingly interconnected, compromise propagates across identity systems, transaction engines, payment channels, and customer interfaces, producing cascading financial and regulatory consequences. By the time impact is fully visible, the window for strategic decision-making has already closed.

What SecureBank Changes

SecureBank reframes cyber risk as a **systemic financial exposure**, not a technical anomaly. Rather than static assessments, the framework models how compromise propagates through interconnected systems, how losses accumulate over time, and when regulatory thresholds are crossed.

The result is **decision-grade intelligence**, not security telemetry.

How the Framework Works

SecureBank operates as a five-layer decision framework:

- **Threat Propagation** — models direction, velocity, and reach across functional zones.
- **Systemic Dependencies** — identifies amplification points, bottlenecks, and cascade paths.
- **Impact Quantification** — computes expected loss and maximum plausible loss by zone and time window.
- **Regulatory Exposure** — aligns loss trajectories with notification thresholds and supervisory escalation.
- **Decision & Resilience** — ranks options by systemic risk reduction per dollar invested and defines actionable targets.

What Executives Gain

SecureBank enables leadership:

- Compare security investments using **financial impact**, not control counts.
- Identify architectures that **amplify or contain systemic loss**.

- Understand **time-critical escalation paths** before incidents occur.
- Support decisions with **documented, defensible assumptions**.
- Align cyber decisions with **capital, resilience, and regulatory accountability**.

Governance Impact

SecureBank produces a structured decision record linking technical signals to financial exposure and regulatory obligations, supporting board oversight, audit readiness, and supervisory review.

Next Step

Apply SecureBank to a defined high-exposure scope using realistic scenarios and institution-specific data to establish a decision baseline for future investments and resilience planning.

Abstract

Cybersecurity decisions in financially regulated environments remain largely guided by compliance metrics and control maturity assessments. While these instruments support audit readiness, they frequently fail to quantify systemic financial and regulatory exposure under realistic cyber failure scenarios. This paper introduces SecureBank™, a systemic cyber risk modeling framework designed to quantify threat propagation through transactional environments and translate technical events into decision-grade financial loss, regulatory exposure, and resilience trade-offs. SecureBank is structured as a five-layer architecture that models propagation dynamics, systemic dependencies, impact quantification, regulatory exposure, and comparative decision outcomes, enabling boards and executive leadership to evaluate options based on systemic risk reduction per dollar invested. The framework is designed to operate in AI-enabled ecosystems while explicitly separating automation from accountability through transparent logic, explicit assumptions, and defensible decision records.

Keywords: systemic cyber risk; financial sector; cyber risk quantification; operational resilience; regulatory exposure; decision-grade intelligence; threat propagation.

Contents

1. Executive Summary

Cybersecurity decisions in financially regulated environments are still predominantly guided by compliance metrics, control maturity assessments, and qualitative risk classifications. While these instruments support audit readiness, they fail to address the question that ultimately governs executive accountability: **how much financial and regulatory exposure an institution faces under a realistic cyber failure scenario**.

As modern banking architectures become increasingly interconnected, cyber incidents no longer remain confined to isolated technical domains. Compromise events propagate rapidly across identity platforms, transaction authorization flows, payment channels, and customer-facing services, generating cascading financial, operational, and regulatory consequences. Existing risk approaches do not adequately model this propagation, nor do they translate technical failures into decision-grade financial exposure.

SecureBank addresses this gap by introducing a **systemic cyber risk modeling framework** designed to quantify how cyber threats propagate through transactional environments and materialize as financial and regulatory impact over time. Rather than focusing on control enumeration or static compliance states, SecureBank models institutions as interconnected systems whose behavior under stress determines loss magnitude, escalation speed, and regulatory outcome.

At its core, SecureBank enables executives, boards, and CISOs to move from abstract risk discussions to **measurable, comparable, and defensible decisions**. The framework translates cyber scenarios into expected loss, maximum plausible loss, regulatory exposure, and comparative resilience outcomes across alternative architectures and mitigation strategies. This allows leadership to evaluate security investments based on **systemic risk reduction per dollar invested**, rather than on compliance alignment alone.

Structured as a five-layer architecture, SecureBank progressively transforms technical signals into executive decisions. Early layers model threat propagation and systemic dependencies, while later layers quantify financial loss, assess regulatory exposure, and rank strategic options under real-world constraints. This layered structure ensures traceability between technical events and board-level decisions—an essential requirement in regulated environments.

Designed for AI-enabled ecosystems, SecureBank explicitly separates **automation from accountability**. Analytical models and AI-driven tools may inform individual layers, but final decisions remain governed by transparent logic, explicit assumptions, and documented trade-offs. This ensures that decisions informed by SecureBank are explainable, auditable, and defensible to regulators, auditors, and external stakeholders.

By reframing cyber risk as a measurable financial and regulatory variable, SecureBank empowers institutions to make informed decisions **before incidents occur**—when those decisions can still prevent cascading failure rather than merely explain it after the fact.

2. The Decision Gap in Cyber Risk

Despite significant investment in cybersecurity, most financial institutions continue to make critical security decisions without a clear understanding of their systemic financial consequences. Boards and executive committees routinely approve security budgets, architectural changes, and risk acceptances based on compliance posture, control coverage, and qualitative assessments, rather than on quantified exposure to loss.

This creates a persistent decision gap. While technical teams can describe vulnerabilities and controls in detail, executive leadership lacks a reliable mechanism to assess how a cyber failure would propagate across interconnected systems and materialize as financial, operational, and regulatory damage. Cyber risk therefore remains abstract at the decision level, disconnected from capital allocation and strategic planning.

In contemporary financial architectures, risk rarely originates or remains within a single system. Identity services, payment rails, transaction engines, customer channels, and third-party integrations form tightly coupled environments where localized compromise can escalate rapidly. Existing decision processes seldom capture this chain reaction in a measurable and time-aware manner.

The reliance on static assessments exacerbates this gap. Point-in-time evaluations and maturity scores describe the presence of controls, but not the behavior of systems under stress. They fail to answer how quickly losses accumulate once controls fail, or when escalation becomes irreversible.

Executives are thus held accountable for outcomes—financial loss, regulatory sanctions, systemic disruption—while being forced to decide using instruments that do not quantify those outcomes in advance. Security investments are justified retrospectively, after incidents occur, rather than proactively based on comparative reduction of systemic exposure.

3. Limitations of Existing Approaches

Existing cyber risk frameworks provide valuable structure for governance and audit alignment, yet they remain fundamentally limited when applied to systemic decision-making. Most were designed to ensure consistency and minimum security baselines, not to support executive decisions under conditions of cascading failure and financial exposure.

A primary limitation is their control-centric orientation. These approaches assume that stronger controls directly translate into lower risk. While valid at a technical level, this assumption breaks down in interconnected financial environments where the failure of a single control can rapidly propagate across multiple systems.

Another critical limitation is the absence of propagation modeling. Risks are evaluated in isolation, within predefined system boundaries, without accounting for how compromise in one domain accelerates exposure elsewhere. As a result, both the speed and magnitude of real-world impact are consistently underestimated.

Financial translation remains insufficient. Static estimates or annualized loss figures fail to

capture temporal dynamics, dependency effects, and concentration of exposure. They do not reflect how loss accumulates minute by minute, nor how architectural choices materially alter outcomes.

Regulatory defensibility is also weakly addressed. While compliance mapping is supported, few frameworks provide structured justification for why risks were accepted, why certain mitigations were prioritized, or how decisions balanced financial exposure against regulatory expectations.

These limitations do not diminish the value of existing frameworks; rather, they define the boundaries of what those frameworks were designed to achieve. SecureBank is intentionally positioned beyond those boundaries, focusing on system behavior, financial consequence, and defensible decision-making.

4. SecureBank Framework Overview

SecureBank is a systemic cyber risk modeling framework designed to support executive decision-making in financially regulated environments. It focuses on how cyber failures propagate through interconnected systems and materialize as financial and regulatory consequences over time.

The framework is built on the premise that cyber risk is not an isolated technical event, but a dynamic system behavior. Identity platforms, transaction flows, devices, channels, and operational zones form coupled architectures where localized compromise can escalate into systemic loss.

SecureBank operates above existing security standards and analytical tools, integrating their outputs into a structured model that produces decision-grade intelligence. It does not replace detection, monitoring, or compliance mechanisms; it governs how their outputs are interpreted and used.

Structured as a five-layer architecture, SecureBank progressively transforms technical signals into executive decisions, ensuring traceability between events, financial exposure, regulatory impact, and chosen responses.

5. The Five-Layer Architecture

5.1 Layer 1: Threat Propagation

The first layer models how compromise signals initiate and expand across functional zones, capturing direction, velocity, and affected transactional surfaces. Its output is a propagation map that establishes time-sensitive exposure boundaries for subsequent dependency and loss modeling.

5.2 Layer 2: Systemic Dependencies

The second layer maps technical and operational interdependencies across identity, transaction processing, devices, channels, and functional zones. It identifies amplification points, containment bottlenecks, and cascade paths that explain why and where propagation accelerates.

5.3 Layer 3: Impact Quantification

The third layer translates propagation dynamics into expected loss and maximum plausible loss by scenario, segmented by zone and time window. Loss is treated as an accumulating exposure curve shaped by propagation velocity, transactional concentration, and containment effectiveness.

5.4 Layer 4: Regulatory Exposure

The fourth layer aligns loss trajectories with regulatory obligations, notification thresholds, and supervisory consequences. Outputs include a regulatory exposure profile that supports auditability and defensibility across incident timelines.

5.5 Layer 5: Decision & Resilience

The fifth layer integrates financial and regulatory outputs with cost and feasibility constraints to rank strategic options by systemic risk reduction per dollar invested. It produces actionable resilience targets and predefined response triggers suitable for board-level governance.

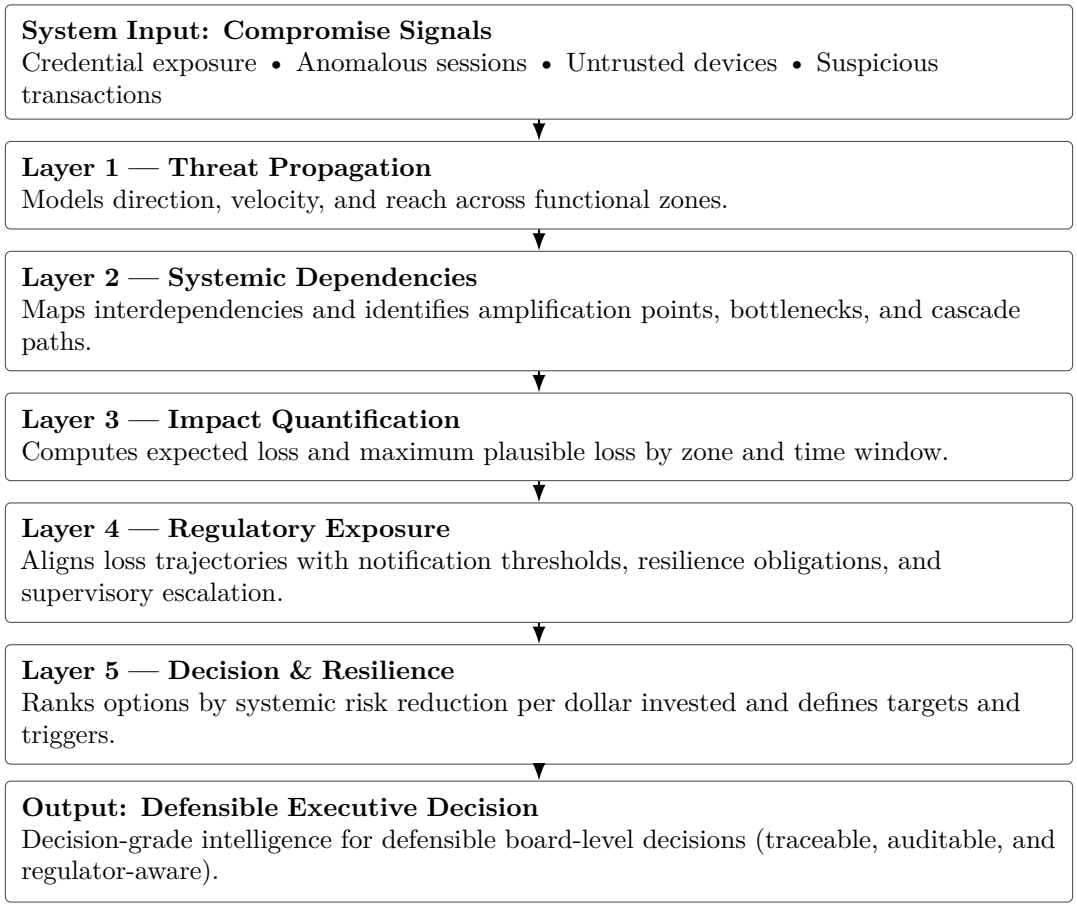

Figure 1: SecureBank™ five-layer architecture: translating compromise signals into decision-grade financial and regulatory outcomes.

6. Financial & Regulatory Translation

SecureBank bridges the gap between technical analysis and executive accountability by translating cyber events into financial exposure and regulatory consequence. Loss is treated as an accumulating function over time, aligned with regulatory timelines and defensibility requirements.

Decisions are documented within a consistent analytical structure, creating a defensible decision record suitable for governance, audit, and supervisory review.

7. Applied Hypothetical Scenario

A mid-sized financial institution operating a digital banking platform detects anomalous authentication behavior. SecureBank models propagation, dependency amplification, loss accumulation, regulatory escalation, and response options, identifying a strategy that limits both financial loss and supervisory exposure despite higher short-term operational cost.

This scenario illustrates how SecureBank transforms early technical signals into time-sensitive, financially grounded, and regulator-aware decisions.

8. Implications for Decision-Makers & Next Steps

SecureBank enables boards, CISOs, and compliance leaders to govern cyber risk as a strategic financial variable rather than a reactive technical concern. The framework supports proactive investment decisions, defensible risk acceptance, and measurable resilience planning.

The next step for institutions is to apply SecureBank to a defined scope using realistic scenarios and institution-specific data, establishing a decision baseline for future investments and governance.

A. Appendix A: Formalizing Propagation and Dependency Modeling

A.1 Propagation primitives

(Optional) Define compromise signals, states, and transition rules used to estimate propagation velocity across zones.

A.2 Dependency graph representation

(Optional) Formalize the dependency graph, including amplification points, containment bottlenecks, and cascade path identification.

B. Appendix B: Financial Loss Assumptions and Scenario Design

B.1 Loss components

(Optional) Define fraud loss, service disruption loss, remediation cost, and secondary financial impacts.

B.2 Time-window modeling

(Optional) Describe how loss accumulates over discrete time windows under different containment strategies.

C. Appendix C: Regulatory Mapping and Defensibility Model

C.1 Regulatory obligations mapping

(Optional) Map scenario outputs to notification timelines, reporting thresholds, and resilience requirements.

C.2 Defensibility record structure

(Optional) Define what a defensibility record contains and how it supports audits and post-incident review.

D. Appendix D: AI-Enabled Environments (Automation vs Accountability)

D.1 Where AI informs the framework

(Optional) Describe where analytics/AI can support detection, correlation, and estimation without owning accountability.

D.2 Auditability and transparency

(Optional) Define constraints, assumptions, and traceability requirements for AI-informed outputs.