Escalation of Ransomware-as-a-Service (RaaS) Attacks on Financial Institutions and Optimizing Cybersecurity Investment: A Quantitative Decision and Risk Perspective

Ashish Dutt (ad4518)

TMGTPS5136_004_2025_3 – Cybersecurity

Professor Cristina Dolan

November 9, 2025

Table of Contents

Abstract

The financial sector is facing an escalation of Ransomware-as-a-Service (RaaS) attacks, resulting in growing operational, regulatory, and reputational risks. As financial institutions expand their digital infrastructures, the key challenge has shifted from whether to invest in cybersecurity to determining how much to invest and how best to allocate limited resources. This paper examines cybersecurity investment decision-making in financial institutions through a quantitative decision and risk framework. Using publicly available data from industry reports, including IBM, PwC, and ENISA, the study develops an exponential cybersecurity investment and risk-cost optimization model to analyse the relationship between spending, expected loss, and total cost. The results reveal a point of diminishing returns, where total cost initially decreases with increased investment but begins to rise beyond an optimal threshold. The findings highlight the importance of aligning cybersecurity budgets with institutional risk appetite and regulatory expectations. By integrating principles of decision science, operational risk management, and cybersecurity economics, this study contributes to the ongoing academic and practical discussions on data-driven cybersecurity investment strategies in the financial sector.

1. Introduction

The financial sector has become a prime target for Ransomware-as-a-Service (RaaS) and other large-scale cyberattacks. According to IBM's Cost of a Data Breach Report (2025), financial services continue to face some of the highest breach costs worldwide, averaging more than 5.56 million dollars per incident. As digital transformation accelerates and institutions adopt cloud and AI-driven platforms, the complexity of their cyber risk landscape continues to grow.

Despite stronger awareness and increasing regulatory oversight, from the U.S. Securities and Exchange Commission's cybersecurity disclosure requirements to the Basel Committee's operational risk standards, financial institutions still face a fundamental strategic question: how much should be invested in cybersecurity, and where should that investment be directed to achieve effective protection?

This challenge sits at the intersection of finance, operations, and decision science. Overinvesting can strain budgets and lead to diminishing returns, while underinvesting leaves organizations vulnerable to financial, legal, and reputational damage.

To address this challenge, this study applies an Exponential Cybersecurity Investment and Risk-Cost Optimization Model adapted from the Gordon - Loeb framework. The model quantifies the relationship between cybersecurity spending, expected loss, and residual risk to identify the point of diminishing returns and propose a framework for data-driven, cost-effective decision-making. By framing cybersecurity as an economic optimization problem, the paper provides a data-driven approach to help executives and risk officers align cybersecurity budgets with enterprise risk appetite, regulatory expectations, and operational resilience.

2. Overview of Cybersecurity Landscape

2.1. Financial Sector Challenge and Operational Impact

Financial institutions, in particular, face unique challenges due to their high-value digital assets, complex IT infrastructures, and stringent regulatory requirements. The contemporary threat landscape has shifted the focus from simple data theft to high-impact operational and systemic risk**,** where disruption can halt critical market functions.

The reality of this operational threat is demonstrated by the EquiLend ransomware attack in January 2024. This incident forced the Wall Street securities finance platform to take core client-facing trading services offline for nearly two weeks. Given the platform's critical role in facilitating trillions in monthly transactions, this systemic outage confirms that a failure in a single key institution can generate severe, multi-party economic consequences. This evidence thus validates and justifies the high baseline cost per breach (C_0) assumptions utilized in contemporary quantitative risk models.

2.2. The Economic Problem and Gaps

Consequently, Scholars and industry practitioners alike have emphasized that the problem of cybersecurity is no longer solely technical - it is fundamentally an economic and strategic decision problem (Gordon & Loeb, 2002). The Gordon - Loeb model remains one of the most influential frameworks in this domain, demonstrating that organizations should not necessarily spend the maximum possible amount on cybersecurity but rather an optimal proportion of expected loss to minimize total cost. Subsequent studies have extended this model to incorporate uncertainty, game theory, and risk-based prioritization, offering quantitative methods for determining how much and where to invest in security controls. These approaches align with the decision and risk operations perspective, where optimal resource allocation is derived from balancing investment cost against residual risk exposure.

However, despite the strength of this academic foundation, a persistent gap remains: according to PwC's *Global Digital Trust Insights* (2026), over 60% of financial institutions plan to increase cybersecurity budgets, yet fewer than half employ formalized models to evaluate investment efficiency. Reports by IBM (2025) and ENISA (2025) similarly emphasize that while spending is rising, many organizations fail to link investment decisions to measurable reductions in cyber risk. Regulatory developments, including the U.S. SEC's cybersecurity disclosure requirements and the Basel Committee's guidance on operational resilience, further underscore the necessity of a quantifiable, evidence-based approach. This paper seeks to bridge that gap by applying a quantitative modelling approach to simulate how investment decisions affect risk reduction and total cost in financial institutions. In doing so, it contributes to both academic research and practical management frameworks for optimizing cybersecurity resource allocation under uncertainty.

3. Analysis and Results: A Quantitative Decision Framework

The assessment of cybersecurity risk within financial institutions must extend beyond qualitative description to include rigorous, quantitative analysis that guides investment strategy. While inherent vulnerabilities (technical debt, human error, third-party vendor risk) define the risk landscape, the risk-cost trade-off model developed in this paper provides the essential framework for determining the optimal resource allocation to mitigate them.

This study adopts a quantitative modelling approach to examine how financial institutions can optimize cybersecurity investments to minimize total risk-related costs. The model integrates elements of decision science and risk management, using cost–benefit analysis to identify the optimal level of investment under conditions of uncertainty. It is conceptually grounded in the Gordon - Loeb model (2002), which suggests that an organization's optimal cybersecurity investment should not exceed a specific fraction of the expected loss from a potential breach.

3.1. Cybersecurity Investment and Risk-Cost Optimization Model Framework

The model evaluates the relationship between cybersecurity investment and residual risk through the following functional relationships:

i. Expected Loss (without investment):

   ($L_0 = P_0 * C_0$)

   where (P_0) is the baseline probability of a successful cyber incident, and (C_0) is the estimated cost per incident.

ii. Risk Reduction Function:

   ($R = R_{max} * (1 - e^{-kI}$)

   where (R_{max}) represents the maximum achievable risk reduction, (k) is the efficiency constant reflecting the effectiveness of security controls, and (I) is the level of investment.

iii. Residual Expected Loss:

   ($L = L_0 * (1 - R)$)

iv. Total Cost Function:

   ($T = I + L$)

   where (T) represents total expected cost (the sum of investment cost and residual risk loss).

The optimal investment corresponds to the minimum value of (T), where the marginal benefit of additional investment equals its marginal cost.

3.2. Data and Assumptions

Publicly available data were used to define baseline parameters:

i. (C_0= \$4,440,000) - global average cost breach cost per incident (IBM, 2025).
ii. ($P_0 = 0.15$) - baseline annual breach probability (ENISA, 2025).
iii. ($R_{max} = 0.9$) - representing a 90% theoretical maximum reduction in risk.
iv. ($k = 0.000002$) - derived as an efficiency parameter based on observed spending patterns in financial services (PwC, 2026).

The baseline breach probability (P_0) represents the expected likelihood of a successful cyber incident within a financial institution in the absence of additional protective investment. Although no single public dataset provides a definitive figure, estimates were triangulated using multiple industry reports. The *European Union Agency for Cybersecurity (ENISA) Threat Landscape for the Finance Sector* (2025) identifies financial services as one of the most frequently targeted industries, reporting rising incident rates and exposure to ransomware, phishing, and third-party breaches. Similarly, IBM's *Cost of a Data Breach Report* (2025) ranks financial services among the top three sectors globally in both breach frequency and cost severity. Based on these indicators and consistent with prior modelling in cybersecurity economics, a baseline annual breach probability of ($P_0 = 0.15$) was adopted. This represents a medium-risk scenario that aligns with observed incident recurrence within the financial sector.

The baseline breach cost (C_0 = \$4,440,000) represents the global average cost per incident as reported in IBM's *Cost of a Data Breach Report* (2025). This value serves as the foundation for estimating expected loss prior to the application of risk mitigation measures.

The maximum achievable risk reduction (R_{max}= 0.9) represents a 90% theoretical upper bound on risk mitigation effectiveness. This parameter reflects the realistic limit of protection attainable through cybersecurity investment, acknowledging that residual risk cannot be completely eliminated.

The efficiency constant (k) quantifies how effectively cybersecurity investments reduce residual breach probability. Publicly available industry reports describe spending patterns but do not provide explicit efficiency coefficients; thus, (k) was derived through calibration informed by observed data and theoretical precedent. PwC's *Global Digital Trust Insights* (2026) and IBM (2025) both indicate that financial institutions allocate roughly 8 - 12 percent of IT budgets to cybersecurity, producing measurable yet diminishing returns in risk reduction. Building on the economic framework introduced by Gordon and Loeb (2002) and subsequent refinements by Bohme and Schwartz (2010), efficiency parameters for cybersecurity investment typically range between ($5*10^{-7}$) and ($1*10^{-6}$). Accordingly, this study adopts ($k = 2*10^{-6}$) as a value that reflects medium efficiency consistent with industry practice.

Sensitivity testing for $P_0 = 0.15$ and $P_0 = 0.20$ and k between $1*10^{-6}$ and $3*10^{-6}$confirmed that this assumption yields stable model behaviour. Together, these parameter choices ensure that the model remains theoretically sound and practically grounded in sector-specific data, enabling realistic simulation of the trade-off between cybersecurity investment and residual risk within financial institutions.

3.3. Analytical Procedure

An Excel-based simulation was developed to calculate total cost values across a range of investment levels (from \$0 to \$300,000, in \$5,000 increments). The results were plotted to visualize the trade-off between investment and total cost, allowing identification of the point of diminishing returns. Sensitivity analyses were also performed by adjusting (P_0) and (k) to evaluate the model's robustness under different threat scenarios.

Label	Value	Description
C_0	4440000	Average cost per breach (IBM, 2025)
P_0	0.15	Baseline annual breach probability (ENISA, 2025)
R_{max}	0.9	Max possible risk reduction
k	0.000002	Efficiency constant observed spending patterns in financial services (PwC, 2026).
L_0	666000	Baseline expected loss = breach cost × probability (C0*P0)
$L_0*R_{max}*k$	1.1988	Product
I	90660.52823	Optimal Investment (I= 1/k * ln (L0*R_{max}*k)
T	657260.5282	Minimum total cost

Table 3.3.1: Optimal Investment vs. Minimum Total Cost for $k= 2* 10^{-6}$ *and* $P_0 = 0.15$

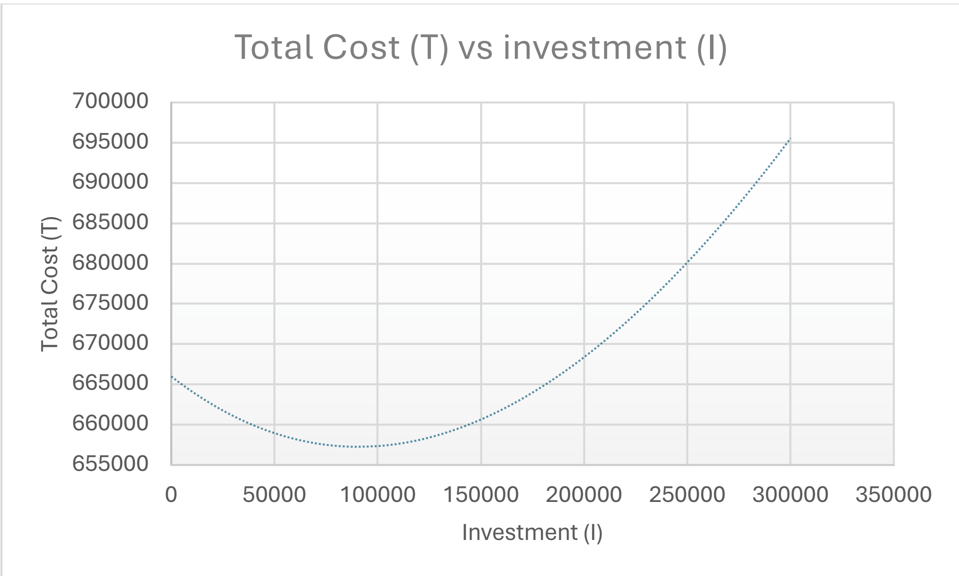
Scenario	k	P0	Optimal Investment (I)	Minimum Total Cost (T)
Low efficiency and medium risk	0.000001	0.15	0	666000
Low efficiency and high risk	0.000001	0.2	0	888000
Medium efficiency and medium risk	0.000002	0.15	90660.52823	657260.5282
Medium efficiency and high risk	0.000002	0.2	234501.5645	823301.5645
High efficiency and medium risk	0.000003	0.15	195595.3882	595528.7215

High efficiency and high risk	0.000003	0.2	291489.4123	713622.7457

Table 3.3.2: Sensitivity Analysis for Optimal Investment vs. Minimum Total Cost

3.4. Identification of the Optimal investment Point

The simulation produced a non-linear relationship between cybersecurity investment and total expected cost, confirming the principle of diminishing returns. As investment increases, the expected loss from cyber incidents declines exponentially, while the total cost initially falls and later rises after reaching an optimal point.



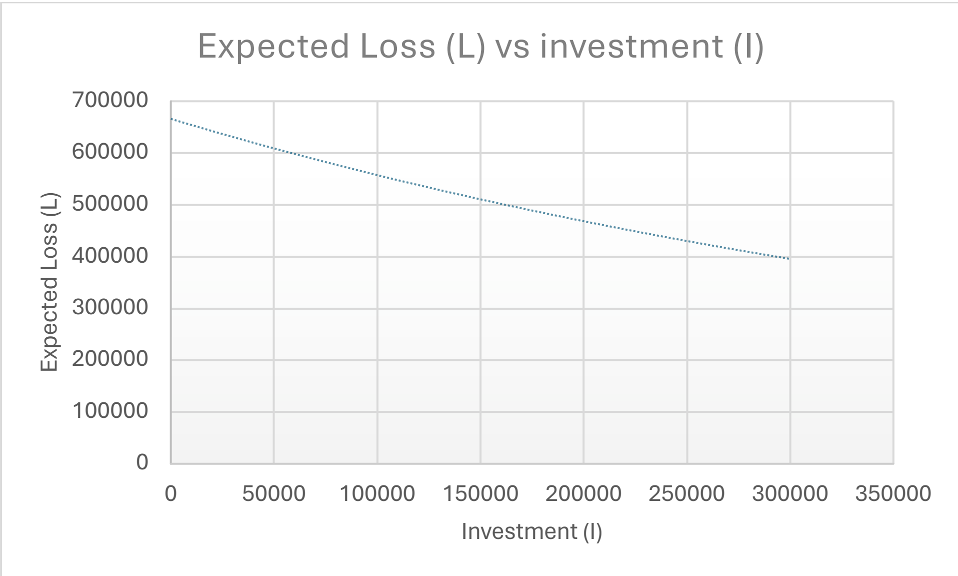
Graph 3.4.1: Total Cost (T) vs. Investment (I)

The total cost curve is typically U-shaped , demonstrating the trade-off:

For the Medium Efficiency and Medium Risk scenario ($k = 2 * 10^{-6}$ *and* $P_0 = 0.15$), the model identifies the optimal investment point:

- Optimal Investment **(I)**: $90,661
- Minimum Total Cost **(T)**:$657,261

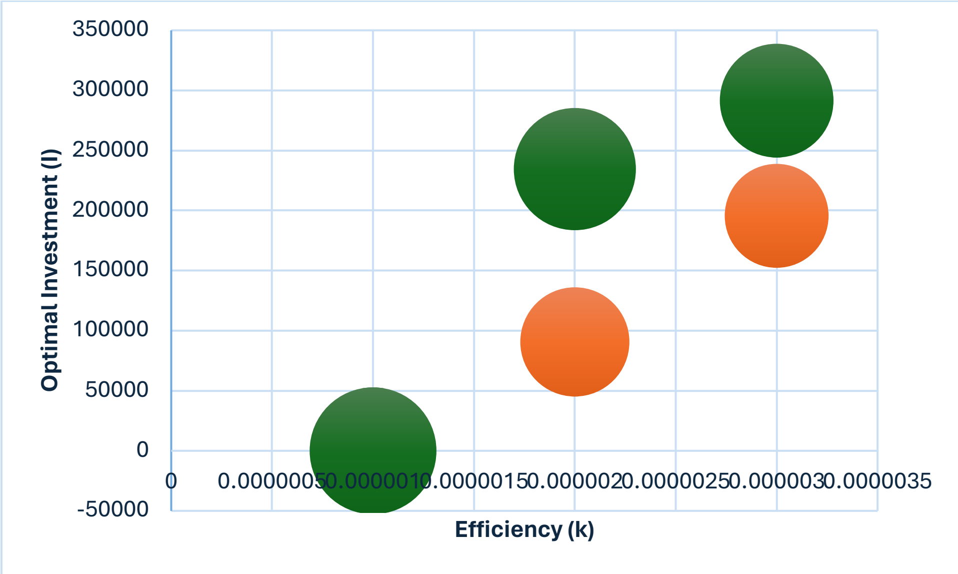
This represents a cost saving of nearly $8,740 compared to the no-investment scenario (L_0 = $666,000), demonstrating that a targeted, optimized investment strategy can yield positive returns.



Graph 3.4.2: Investment (I) vs. Expected Loss (L)

The graph demonstrates how increases in investment are associated with reductions in Expected Loss. This confirms that cybersecurity investment is most valuable when targeted toward high-efficiency controls that rapidly move the organization away from its baseline risk.

3.5. Sensitivity Analysis



Graph 3.5.1: Sensitivity Analysis for Optimal Investment vs. Minimum Total Cost

Sensitivity analysis further supports the robustness of the model. When the baseline breach probability (P_0) or efficiency (k) increases, the optimal investment shifts upward, suggesting that higher exposure justifies higher cybersecurity spending. Conversely, when control efficiency (k) declines, the optimal investment level falls slightly, highlighting the importance of continuously improving security control effectiveness.

4. Detection and Response Strategies

The findings highlight the importance of treating cybersecurity investment as a quantitative optimization problem rather than a purely reactive or compliance-driven activity. Financial institutions often allocate cybersecurity budgets based on regulatory expectations or industry benchmarks; however, this study demonstrates that such decisions should be grounded in measurable risk-reduction outcomes. Consequently, Detection and Response (D&R) is not merely a technical function but a strategic mechanism designed to optimize k, maximizing the risk reduction achieved per dollar spent. D&R strategies must, therefore, be aligned with the organization's calculated optimal investment I.

4.1. Technology and Process: Drivers of I and k

Investment in D&R systems constitutes the Investment I component of the total cost function, while the processes utilizing these systems primarily define the efficiency constant k. The optimal approach focuses on high k returns for both technology acquisition and operational speed.

D&R Component	Primary Impact	Quantitative Rationale
SIEM & EDR Tools	Investment (I)	These tools must be selected based on their potential to provide the widest visibility to justify the initial cost I.
Containment Automation (SOAR)	Efficiency (k)	Automation directly boosts k. By reducing the time-to-contain (TTC) from hours to minutes, SOAR minimizes the final incurred loss and ensures the marginal benefit of investment remains high.
Response Playbook	Efficiency (k)	Well-tested playbooks are a non-monetary investment that ensures consistency. This operational readiness stabilizes and maximizes k, preventing inefficient spending.

Recovery Procedures	Expected Loss (L)	Focuses on minimizing system downtime and data loss, which are the largest drivers of the breach cost C_0. Rapid recovery directly limits the maximum potential expected loss L.

Table 4.1.1: D&R Component, Primary Impact and Quantitative rationale

4.2. Optimal Organisational Structure Aligned with I

The structure of the Computer Incident Response Team (CIRT) must be scaled to reflect the calculated I from the optimization model:

i. Sub - critical Efficiency (When I=0):

When k is too low, the marginal cost of investment exceeds the benefit. The organization should adopt a lean, cross-functional structure and rely on managed security services (MSSP**).** Investment (I) is minimized by leveraging cloud-native tools and simple scripting rather than costly, dedicated internal staff or proprietary SIEM systems. The focus is exclusively on process improvement to raise k above the critical threshold before justifying new capital.

ii. Critical Efficiency (When I>0):

When k is high enough to generate savings, the organization is justified in making the optimal investment I. This requires a dedicated, specialized 24/7 CIRT capable of threat hunting and advanced forensics. The cost of these human resources is offset by the substantial reduction in expected loss achieved through their high-efficiency operations.

By aligning D&R strategy with the efficiency constant k and the optimal investment I, organizations can transform cybersecurity from a generic expense into a data-driven, cost-reduction strategy.

5. Policy, Governance and Compliance

Policy, governance, and compliance (PGC) translate the analytical finding of the Optimal Investment I into an actionable, enforced mandate. The governance structure is responsible for setting the financial and risk parameters of the organization, which are the inputs P_0 , C_0 to the total cost function. Compliance ensures that a minimum floor for investment is met, even in scenarios where the mathematical optimum is I=0.

5.1. Governance: Defining Inputs and Allocating I

Governance is the mechanism by which executive leadership sets the key inputs for our risk calculation. The Board's primary function in this context is twofold:

i. Setting P_0: The Board defines the organizational risk appetite. This decision directly translates into the Baseline Probability P_0 of a material breach, which is the foundational input for the expected loss calculation. Governance formally accepts or rejects the initial risk position.
ii. Mandating I**:** Once the CISO calculates the Optimal Investment I required to reach the minimum total cost point, governance ensures that budget is allocated for this specific expenditure.

If governance fails to set clear risk parameters, the model's output becomes irrelevant, as there's no authority to fund it or enforce its underlying risk assumptions.

5.2. Compliance and Policy: Influencing C_0 and k

Compliance and internal policies play the critical role of adjusting the cost function and maximizing the efficiency of spending.

i. Impact on Breach Cost **(**C_0): Regulations like GDPR or PCI-DSS don't necessarily prevent attacks, but they drastically increase the financial Cost of a Breach through regulatory fines and legal liabilities. This external compliance constraint pushes the overall expected loss up, which in turn mathematically necessitates a higher Optimal Investment **(**I) to return to the minimum total cost curve.

ii. Maximizing Efficiency (k): Internal policies are essential for maximizing the Efficiency Constant**.** For example, a robust "Vulnerability Patching Policy" ensures that the money spent on vulnerability scanners (I) actually translates into real risk reduction (high k). Without a strong policy, investment is inefficient, potentially leading to the I=0 scenario we observed in the low-efficiency cases.

Ultimately, effective Policy, Governance, and Compliance ensures that the financial optimal investment (I) is not just a theoretical number, but a mandatory expenditure supported by enforceable policies and accountability structures.

6. Discussions and Recommendations

The quantitative findings derived from the optimization model lead to three core, actionable recommendations for Chief Information Security Officers (CISOs), risk officers, and governance bodies within the financial sector. These recommendations confirm the Gordon-Loeb principle, advocating for an economically rational approach to cybersecurity investment.

6.1. Implement an Economically Optimal Budgeting Cycle

Financial institutions must abandon flat or historical budgeting methods and transition to an evidence-based investment cycle.

i. Mandate I Calculation**:** The CISO should use the derived Optimal Investment **(**I) as the foundation for the annual cybersecurity budget, spending only the fraction of the expected loss that minimizes the total cost function (T).

ii. Establish Total Cost Targets: Governance must accept the resulting Minimum Total Cost as the calculated risk target, ensuring resources are not over-spent beyond the point of diminishing returns. This directly links cybersecurity spending to measurable reductions in expected financial loss, improving transparency.

6.2. Prioritize Operational Efficiency (k)

The model's sensitivity analysis confirmed that the Efficiency Constant (k), the effectiveness of the investment, is the most critical variable.

i. Fund Process Automation First: Capital investment priority must shift away from acquiring siloed systems toward optimizing the operational efficiency of existing security controls. This includes funding projects that improve Mean Time to Detect (MTTD) and Mean Time to Contain (MTTC), such as Security Orchestration, Automation, and Response (SOAR) technologies and staff training.

ii. Measure k Directly: Organizations must develop internal metrics to quantify k before approving major projects, ensuring that capital spending demonstrably enhances the efficiency of the security response mechanism rather than merely increasing the overall investment (I).

6.3. Integrate Model into Enterprise Risk Governance

The model offers practical value by enabling risk officers to formally integrate cybersecurity resource allocation into the broader Enterprise Risk Management (ERM) framework.

i. Link Spending to Risk Appetite: Integrate the model's inputs, specifically the Baseline Probability **(**P_0) and Cost of Breach (C0) directly into organizational risk appetite statements. This formal linkage enhances accountability and better aligns cybersecurity investment with strategic business priorities.
ii. Improve Reporting Transparency: Utilize the output (Expected Loss and Total Cost) to report the true financial impact of cybersecurity to the Board and regulators, providing a clear, quantitative justification for budgetary decisions and demonstrating operational resilience.

7. Conclusion and Future Research

This paper has demonstrated the value of integrating principles from financial economics into cybersecurity decision-making. By operationalizing the Gordon-Loeb model within a framework for financial institutions, we derived a concrete method for calculating the Optimal Investment (I) required to achieve the Minimum Total Cost**.**

The core insight is clear: cybersecurity spending is an optimization problem, not a defensive imperative. Organizations should spend only a justifiable fraction of their expected loss, but only if that investment can be executed with sufficient Efficiency **(**k**)**. Our sensitivity analysis proved that when operational efficiency is low, the mathematically sound decision is to invest nothing until processes are improved.

Ultimately, these findings advocate for a fundamental shift in technology management: moving from reactive, compliance-driven budgeting to a data-driven, economically rational governance model**.** This approach not only provides the quantitative basis to justify resource allocation to the Board and regulators but also ensures that every dollar spent maximizes the reduction in true financial risk, thereby enhancing enterprise resilience.

Further work can explore Game Theory models and non-exponential risk reduction functions.

8. References

[1] Basel Committee on Banking Supervision. (2011, June). *Principles for the sound management of operational risk and the role of supervision* (BCBS 195). Bank for International Settlements. https://www.bis.org/publ/bcbs195.pdf

[2] Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security, 5*(4), 438–457. https://doi.org/10.1145/581271.581274

[3] IBM. (n.d.). *What is ransomware as a service (RaaS)?* Retrieved November 9, 2025, from https://www.ibm.com/think/topics/ransomware-as-a-service

[4] Imagine IT. (2025, September 9). *How to protect banks from ransomware attacks in 2025?* https://imit.com/ransomware-attacks-on-banks/#:~:text=Q1.,information%20and%20cause%20financial%20losses

[5] Matthews, L. (2024, February 26). EquiLend hack raised costs as traders flew blind, sources say. *Reuters.* https://www.reuters.com/technology/cybersecurity/equilend-hack-raised-costs-traders-flew-blind-sources-say-2024-02-26/

[6] PwC. (2025, October 1). *2026 Global Digital Trust Insights Survey: C-suite playbook and findings.* https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html

[7] European Union Agency for Cybersecurity (ENISA). (2025, October 1). *ENISA Threat Landscape 2025*. https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025.pdf

[8] IBM & Ponemon Institute. (2025). *Cost of a Data Breach Report 2025: The AI oversight gap* [PDF]. https://www.ibm.com/downloads/documents/us-en/131cf87b20b31c91

9. Optional Appendices

	A	B	C	D
11	Investment (I)	Risk Reduction (R)	Expected Loss (L)	Total Cost (T)
12	0	0	666000	666000
13	5000	0.00895515	660035.8703	665035.87
14	10000	0.017821194	654131.0848	664131.08
15	15000	0.02659902	648285.0528	663285.05
16	20000	0.035289505	642497.1898	662497.19
17	25000	0.043893518	636766.917	661766.92
18	30000	0.05241192	631093.6614	661093.66
19	35000	0.060845562	625476.8557	660476.86
20	40000	0.069195288	619915.938	659915.94
21	45000	0.077461933	614410.3525	659410.35
22	50000	0.085646324	608959.5484	658959.55
23	55000	0.093749278	603562.9807	658562.98
24	60000	0.101771607	598220.1098	658220.11
25	65000	0.109714112	592930.4013	657930.4
26	70000	0.117577588	587693.3263	657693.33
27	75000	0.125362821	582508.3611	657508.36
28	80000	0.13307059	577374.9871	657374.99
29	85000	0.140701665	572292.6911	657292.69
30	90000	0.14825681	567260.9647	657260.96
31	100000	0.163142322	557347.2134	657347.21
32	105000	0.170474179	552464.197	657464.2
33	110000	0.177733082	547629.7675	657629.77
34	115000	0.184919758	542843.4413	657843.44
35	120000	0.192034925	538104.7399	658104.74
36	125000	0.199079295	533413.1894	658413.19
37	130000	0.206053573	528768.3205	658768.32
38	135000	0.212958455	524169.6689	659169.67
39	140000	0.219794633	519616.7746	659616.77
40	145000	0.226562789	515109.1824	660109.18
41	150000	0.233263601	510646.4415	660646.44
42	155000	0.239897739	506228.1056	661228.11
43	160000	0.246465867	501853.7328	661853.73
44	165000	0.25296864	497522.8858	662522.89
45	170000	0.25940671	493235.1315	663235.13
46	175000	0.265780719	488990.041	663990.04
47	180000	0.272091307	484787.1898	664787.19
48	185000	0.278339102	480626.1578	665626.16
49	190000	0.284524732	476506.5287	666506.53
50	195000	0.290648813	472427.8906	667427.89
51	200000	0.296711959	468389.8356	668389.84
52	205000	0.302714775	464391.9599	669391.96
53	210000	0.308657862	460433.8638	670433.86
54	215000	0.314541815	456515.1514	671515.15
55	220000	0.320367221	452635.4308	672635.43
56	225000	0.326134664	448794.3141	673794.31
57	230000	0.331844719	444991.4171	674991.42
58	235000	0.337497959	441226.3596	676226.36
59	240000	0.343094947	437498.765	677498.77
60	245000	0.348636245	433808.2607	678808.26
61	250000	0.354122406	430154.4774	680154.48
62	255000	0.359553979	426537.0499	681537.05
63	260000	0.364931507	422955.6165	682955.62
64	265000	0.370255527	419409.8188	684409.82
65	270000	0.375526573	415899.3025	685899.3
66	275000	0.380745171	412423.7163	687423.72
67	280000	0.385911843	408982.7129	688982.71
68	285000	0.391027105	405575.948	690575.95
69	290000	0.39609147	402203.0809	692203.08
70	295000	0.401105444	398863.7745	693863.77
71	300000	0.406069528	395557.6947	695557.69

Image 9.1: Full Excel Analysis for Total Cost vs Investment for $k = 2*10^{-6}$ and $P_0=0.15$

	A	B	C
1	**Label**	**Value**	**Description**
2	C0	4440000	Average cost per breach (IBM, 2025)
3	P0	0.15	Baseline annual breach probability (ENISA, 2025)
4	Rmax	0.9	Max possible risk reduction
5	k	0.000001	Efficiency constant
6	L0	666000	Baseline expected loss = breach cost × probability (C0*P0)
7	L0*Rmax*k	0.5994	Product
8	I	0	Optimal Investment (I= 1/k * ln (L0*Rmax*k)
9	T	666000	Mimimum total cost

*Image 9.2: Minimum Total Cost and Optimal Investment for k= 1*10^{-6} and P_0=0.15*

	A	B	C
1	**Label**	**Value**	**Description**
2	C0	4440000	Average cost per breach (IBM, 2025)
3	P0	0.2	Baseline annual breach probability (ENISA, 2025)
4	Rmax	0.9	Max possible risk reduction
5	k	0.000001	Efficiency constant
6	L0	888000	Baseline expected loss = breach cost × probability (C0*P0)
7	L0*Rmax*k	0.7992	Product
8	I	0	Optimal Investment (I= 1/k * ln (L0*Rmax*k)
9	T	888000	Mimimum total cost

*Image 9.3: Minimum Total Cost and Optimal Investment for k= 1*10^{-6} and P_0=0.2*

	A	B	C
1	**Label**	**Value**	**Description**
2	C0	4440000	Average cost per breach (IBM, 2025)
3	P0	0.2	Baseline annual breach probability (ENISA, 2025)
4	Rmax	0.9	Max possible risk reduction
5	k	0.000002	Efficiency constant
6	L0	888000	Baseline expected loss = breach cost × probability (C0*P0)
7	L0*Rmax*k	1.5984	Product
8	I	234501.5645	Optimal Investment (I= 1/k * ln (L0*Rmax*k)
9	T	823301.5645	Mimimum total cost

*Image 9.4: Minimum Total Cost and Optimal Investment for k= 2*10^{-6} and P_0=0.2*

Label	Value	Description
C0	4440000	Average cost per breach (IBM, 2025)
P0	0.15	Baseline annual breach probability (ENISA, 2025)
Rmax	0.9	Max possible risk reduction
k	0.000003	Efficiency constant
L0	666000	Baseline expected loss = breach cost × probability (C0*P0)
L0*Rmax*k	1.7982	Product
I	195595.3882	Optimal Investment (I= 1/k * ln (L0*Rmax*k)
T	595528.7215	Mimimum total cost

Image 9.5: Minimum Total Cost and Optimal Investment for k= $3*10^{-6}$ and P_0=0.15

Label	Value	Description
C0	4440000	Average cost per breach (IBM, 2025)
P0	0.2	Baseline annual breach probability (ENISA, 2025)
Rmax	0.9	Max possible risk reduction
k	0.000003	Efficiency constant
L0	888000	Baseline expected loss = breach cost × probability (C0*P0)
L0*Rmax*k	2.3976	Product
I	291489.4123	Optimal Investment (I= 1/k * ln (L0*Rmax*k)
T	713622.7457	Mimimum total cost

Image 9.6: Minimum Total Cost and Optimal Investment for k= $3*10^{-6}$ and P_0=0.2