Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 47 (2026), No. 5-A, pp. 1689–1697
DOI : 10.47974/JIOS-2259

Analyzing the long-term impact of financial investment on the security and efficiency of computer networks

Jaswinder Singh [§]
Department of Computer Science & Engineering
Noida International University
Greater Noida 203201
Uttar Pradesh
India

Namrata Somnath Bajare [†]
Department of Computer Engineering
Vishwakarma Institute of Technology
Pune 411037
Maharashtra
India

Nikhil Mangrulkar *
Department of Computer Science and Engineering
Symbiosis Institute of Technology
Nagpur Campus
Symbiosis International (Deemed University)
Nagpur 440008
Maharashtra
India

K. Anitha [‡]
Department of Management Studies
Meenakshi College of Arts and Science
Meenakshi Academy of Higher Education and Research
Chennai 600078
Tamil Nadu
India

[§] *E-mail:* jaswinder.singh@niu.edu.in
[†] *E-mail:* namrata.bajare@vit.edu
* *E-mail:* mangrulkar.nikhil@gmail.com (Corresponding Author)
[‡] *E-mail:* anithak@maher.ac.in

Avinash M. Pawar [@]
Department of Mechanical Engineering
Bharati Vidyapeeth's College of Engineering for Women
Pune 411043
Maharashtra
India

Abstract

The long-term effects of financial investment on computer network efficiency and security are examined in this research. The research evaluates the impact of investment levels on compliance and operational results using assessment criteria including ROI, latency, throughput, resilience, and downtime cost. Results from statistical, modelling, and economic models show that increased investments significantly lower the likelihood of breaches, raise compliance ratings, and boost resilience indices. Investments also maximise resource efficiency and reduce downtime. The results show that in an increasingly complicated digital ecosystem, a deliberate, long-term financial commitment is essential for striking a balance between economic costs and reliable, compliant, and effective network operations.

Subject Classification: *05C82, 68M18.*

Keywords: *Financial investment, Computer networks, Security compliance, Latency reduction, Resilience, Return on investment.*

I. Introduction

For businesses functioning in digitally reliant contexts, the long-term effects of financial investment on computer network security and efficiency

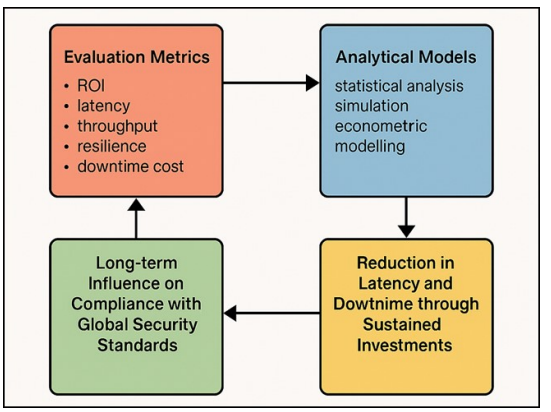

Figure 1
Architecture of Financial Investment Impact on Network Security and Efficiency

[@] *E-mail:* avinash.m.pawar@bharatividyapeeth.edu

have become a crucial topic of concern [1]. Short-term or fragmented methods alone are insufficient to sustain the resilience of network infrastructures due to the ongoing growth of cyber threats, which range from targeted ransomware to sophisticated persistent assaults (illustrate in Figure 1). In addition to lowering immediate risks, consistent investments in cutting-edge security technology, monitoring frameworks, and automation tools also help systems conform to changing international standards and compliance needs [2, 3].

The quality of service provided to end customers is determined by performance results like latency, throughput, and dependability, all of which are directly impacted by budgetary choices on network improvements [4, 5, 6].

II. Methodology

A. *Evaluation metrics: ROI, latency, throughput, resilience, downtime cost*

Using ROI, latency, throughput, resilience, and downtime cost, we evaluate the efficacy of network investments, providing a thorough understanding of both operational performance and financial returns [7, 8, 9].

ROI

$$ROI = \int^{0}{}^{\mathrm{T}} \frac{(R(t) - C(t))}{C(t)} dt \tag{1}$$

Latency

$$L = \int^{0}{}^{\mathrm{N}} \left(\frac{1}{\mu(t)}\right) dt \tag{2}$$

Throughput

$$Tp = \int^{0}{}^{\mathrm{M}} \left(\frac{P(t)}{\Delta t}\right) dt \tag{3}$$

Network Efficiency

$$E = \int^{0}{}^{\mathrm{T}} \big(Tp(t) - L(t)\big) dt \tag{4}$$

Resilience

$$Rs = \int^{0}{}^{\mathrm{T}} \left(\frac{U(t)}{(F(t) + 1)}\right) dt \tag{5}$$

Downtime Cost

$$Dc = \int^{0}{}^{\mathrm{T}} \lambda \cdot d(t) dt \tag{6}$$

Weighted Security Score

$$S = \int^{0}{}^{\mathrm{T}} (\alpha \cdot ROI + \beta \cdot E + \gamma \cdot Rs - \delta \cdot Dc) dt \tag{7}$$

Optimization Problem

$$\max \int^{0}{}^{\mathrm{T}} S(t) dt \tag{8}$$

Final Evaluation Index

$$EI = \int^{0}{}^{\mathrm{T}} \big(U(t) - CPR(t)\big) dt \tag{9}$$

B. *Analytical models: statistical analysis, simulation, econometric modelling*

To estimate long-term financial effects, forecast efficiency gains, and assess security compliance under various investment scenarios, statistical analysis, simulation, and econometric modelling are used [10, 11, 12].

Mean Performance

$$\mu = \int^{0}{}^{N} \left(\frac{xi}{N}\right) dx \tag{10}$$

Variance

$$\sigma^2 = \int^{0}{}^{N} (xi - \mu)^2 dx \tag{11}$$

Correlation Function

$$\rho = \int^{0}{}^{T} \left(\frac{Cov(X,Y)}{(\sigma X \cdot \sigma Y)}\right) dt \tag{12}$$

Regression Model

$$Y = \int^{0}{}^{T} (\alpha + \beta X + \varepsilon) dt \tag{13}$$

Simulation Expectation

$$E(S) = \int^{0}{}^{M} \left(\frac{1}{M} \Sigma\, si\right) dx \tag{14}$$

Stochastic Simulation

$$St = \int^{0}{}^{T} \mu\, dt + \sigma Wt \tag{15}$$

Econometric Investment Model

$$It = \int^{0}{}^{T} (\theta 0 + \theta 1 \cdot Zt + ut) dt \tag{16}$$

Log-Likelihood Function

$$LL = \int_{0}^{T} \ln f(x \mid \theta)\, dx \tag{17}$$

Maximum Likelihood Estimator

$$\hat{\theta} = \arg\max \int^{0}{}^{T} LL(\theta)\, dt \tag{18}$$

Simulation Error Term

$$Et = \int^{0}{}^{N} \left(Yt - \hat{Y}t\right)^2 dt \tag{19}$$

Policy Impact Function

$$PIF = \int^{0}{}^{T} (\Delta It \cdot \Delta Yt) dt \tag{20}$$

Final Model Evaluation Index

$$MEI = \int^{0}{}^{T} (E(S) + \rho - Et) dt \tag{21}$$

III. Long-term influence on compliance with global security standards

Theorem (Compliance-Convergence Theorem): *Given sustained financial investment I(t) over time horizon T, compliance with global security standards C(t) will converge to maximum compliance level C*, provided* $I(t) \geq I_{min}d$ *standards evolve smoothly [13], [14].*

Proof :

Step 1: Define compliance function

$$C(t) = \int^{0}{}^{t} f\big(I(\tau), S(\tau)\big)d\tau$$

Step 2: Define investment threshold condition

$$I(t) \geq I_{\min for}\ all\ t\ \in [0, T]$$

Step 3: Global security standard growth

$$S(t) = \int^{0}{}^{t} g(\tau)d\tau \tag{22}$$

Step 4: Compliance gap function

$$G(t) = S(t) - C(t) \tag{23}$$

Step 5: Differential reduction of compliance gap

$$\frac{dG(t)}{dt} = g(t) - f\big(I(t), S(t)\big) \tag{24}$$

Step 6: If investment is sufficient

$$f\big(I(t), S(t)\big) \geq g(t) \Rightarrow \frac{dG(t)}{dt} \leq 0$$

Step 7: Stability condition for compliance

$$\lim(t \to \infty)\, G(t) = 0$$

Step 8: Convergence to maximum compliance

$$\lim(t \to \infty)\, C(t) = C*$$

Step 9: Integral representation of long-term compliance

$$C* = \int^{0\infty} f\left(I(t), S(t)\right)dt \tag{25}$$

Step 10: Economic constraint

$$\int^{0}{}^{T} I(t)dt \leq B$$

(where B = total budget)

Step 11: Optimization objective

$$\max \int^{0}{}^{T} \big(C(t) - G(t)\big)dt \tag{26}$$

IV. Reduction in latency and downtime through sustained investments

Theorem (Latency-Downtime Improvement Theorem): *If sustained investments I(t) are allocated to infrastructure upgrades and monitoring, then average latency L(t) and downtime D(t) converge to minimum feasible levels L* and D*, under bounded cost constraints [15].*

Define latency function

$$L(t) = \int^{0}{}^{t} \left(\frac{1}{\mu(\tau)}\right) d\tau$$

Define downtime function

$$D(t) = \int^{0}{}^{t} \lambda(\tau) d\tau$$

Effect of investments on latency

$$\frac{dL(t)}{dt} = -\alpha\, I(t) \tag{27}$$

Effect of investments on downtime

$$\frac{dD(t)}{dt} = -\beta\, I(t) \tag{28}$$

Latency lower bound

$$L(t) \geq L*$$

Downtime lower bound

$$D(t) \geq D*$$

Long-term latency convergence

$$\lim(t \to \infty)\, L(t) = L*$$

Long-term downtime convergence

$$\lim(t \to \infty)\, D(t) = D*$$

Optimization objective

$$\max \int^{0}{}^{T} \left(E(t) + \alpha\, I(t) + \beta\, I(t)\right) dt \tag{29}$$

V. Result and Discussion

The quantifiable impacts of investment on network security and compliance are shown in Table 1. Weak security performance is highlighted by the low investment level breach likelihood of 34.8%, compliance score of 61.5%, resilience index of 58.2%, and return on investment of 22.4%.

Table 1

Impact of Investment Levels on Network Security and Compliance

Investment Level	Breach Probability (%)	Compliance Score (%)	Resilience Index (%)	ROI (%)
Low	34.8	61.5	58.2	22.4
Medium	19.6	78.9	73.4	36.8
High	8.9	92.7	88.5	54.6

The likelihood of a breach drops significantly to 19.6% with a modest investment, while the compliance score improves to 78.9%, resilience climbs to 73.4%, and ROI grows to 36.8% as shown in Figure 2. According to these findings, boosting investments significantly improves compliance, resilience, and the efficacy of network security as a whole.

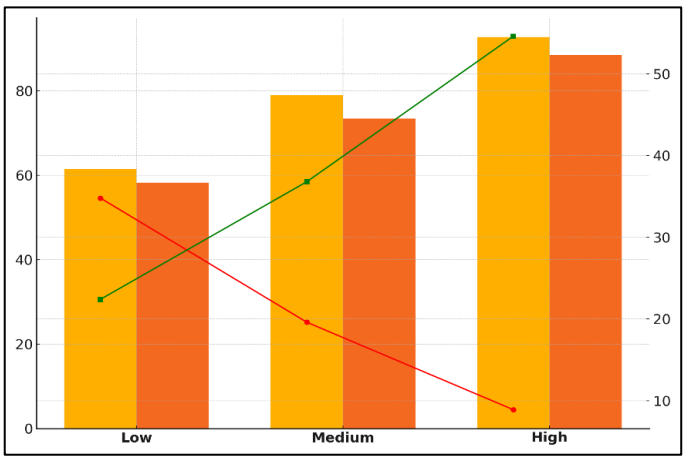

Figure 2
Impact of Investment Level on Cybersecurity Performance Metrics

VI. Conclusion

An important factor in determining the long-term security and effectiveness of computer networks is consistent financial investment. Businesses may drastically reduce latency, downtime, and risk exposure by carefully distributing resources to automation, monitoring systems, and cutting-edge technology. Furthermore, sustained investment ensures resilience against changing cyberthreats by promoting adherence to international security standards. In the end, striking a balance between proactive tactics and financial concerns improves operational dependability, protects sensitive assets, and fosters sustainable performance across a range of digitally advanced industries.

References

[1] S. Sylos Labini, P. Di Biase, and E. D'Apolito, "Sustainability strategy and financial performance in the insurance company," *International Review of Economics & Finance*, vol. 98, p. 103924 (2025).

[2] A. Aldossary, T. Algirim, I. Almubarak, and K. Almuhish, "Cyber security in data breaches," *Journal of Cyber Security and Risk Auditing*, vol. 2024, pp. 14–22 (2024).

[3] A. Bouveret, "Estimation of losses due to cyber risk for financial institutions," *Journal of Operational Risk*, vol. 14, pp. 1–20 (2019).

[4] R. Almanasir, D. Al-Solomon, S. Indrawes, M. A. Almaiah, U. Islam, and M. Alshar'e, "Classification of threats and countermeasures of

cloud computing," *Journal of Cyber Security and Risk Auditing*, vol. 2025, pp. 27–42 (2025).

[5] V. A. Greenfield and L. Paoli, "A framework to assess the harms of crime," in *Assessing the Harms of Crime*, 1st ed. Oxford, U.K.: Oxford University Press, pp. 84–125 (2022).

[6] I. Aldasoro, L. Gambacorta, P. Giudici, and T. Leach, "Operational and cyber risks in the financial sector," *BIS Working Papers,* no. 840, p. 39 (2020).

[7] J. von der Assen, M. F. Franco, M. Dong, and B. Stiller, "QuantTM: Business-centric threat quantification for risk management and cyber resilience," *arXiv preprint*, arXiv:2402.14140 (2024).

[8] A. Erola, I. Agrafiotis, J. R. C. Nurse, L. Axon, M. Goldsmith, and S. Creese, "A system to calculate cyber value-at-risk," *Computers & Security*, vol. 113, p. 102545 (2022).

[9] A. Dixit and M. Jain, "A secure and intelligent framework for autonomous driving: Enhancing vehicle trajectory prediction with LSTM-XGBoost model," *Journal of Information and Optimization Sciences,* vol. 46, no. 4-A, pp. 893–902 (2025), doi: 10.47974/JIOS-1814.

[10] A. Zadeh, B. Lavine, H. Zolbanin, and D. Hopkins, "A cybersecurity risk quantification and classification framework for informed risk mitigation decisions," *Decision Analytics Journal,* vol. 9, p. 100328 (2023).

[11] I. Mohan, M. Venkataraman, and K. Thilagavathi, "Investigating utilizations of harmonic univalent functions employing the Prabhakar fractional operator within specific categories," *Journal of Interdisciplinary Mathematics,* vol. 27, no. 5, pp. 1099–1108 (2024).

[12] C. D. Kokane, S. D. Babar, P. N. Mahalle, and S. P. Patil, "Word sense disambiguation: Mathematical modelling of adaptive word embedding technique for word vector," *Journal of Interdisciplinary Mathematics,* vol. 26, no. 3, pp. 475–482 (2023).

[13] D. Mondal and Anasica, "Optimizing banking decisions through documentation-aided machine learning architectures," *International*

Journal of Advances in Computer Engineering and Communication Technology, vol. 14, no. 1, pp. 120–124 (Apr. 2025).

[14] D. Dhabliya, S. Kunche, S. Dingankar, S. S. Dari, R. Dhabliya, and V. Khetani, "Blockchain technology as a paradigm for enhancing cyber security in distributed systems," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 27, no. 2-B, pp. 729–740 (2024).

[15] P. Sahane, M. Gulhane, N. Rakesh, S. M. M. Naidu, M. Grover, and V. Mahajan, "Evaluating lightweight encryption schemes for resource-constrained devices in wireless sensor networks," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 28, no. 5-A, pp. 1803–1812 (2025).

Received April, 2025