Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 47 (2026), No. 5-A, pp. 1661–1669
DOI : 10.47974/JIOS-2256

Strategic investment approaches for building robust computer security frameworks within organizational networks

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

Amruta Prasad Kharade [†]
Department of Engineering Science and Humanities
Vishwakarma Institute of Technology
Pune 411037
Maharashtra
India

Asha Rawat *
Department of Computer Engineering
NMIMS Deemed-to-be-University
Navi Mumbai 410210
Maharashtra
India

Deepak Suresh Asudani [‡]
Department of Computer Science and Engineering
Symbiosis Institute of Technology
Nagpur Campus
Symbiosis International (Deemed University)
Nagpur 440008
Maharashtra
India

[§] *E-mail:* **veerendra.yadav@niu.edu.in**
[†] *E-mail:* **amruta.kharade@vit.edu**
* *E-mail:* **asha.rawat@nmims.edu (Corresponding Author)**
[‡] *E-mail:* **deepak.s.asudani@gmail.com**

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

Abstract

In order to increase computer security frameworks inside organisational networks, this research offers a structured framework for strategic investment methods. In order to combat emerging cyber threats, proactive and cost-effective solutions are required, since traditional reactive defences are inadequate. The suggested system combines risk-return modelling and mathematical optimisation to direct the effective distribution of scarce resources across many defence layers. Organisations may achieve balanced spending, improved resilience, and quantifiable risk reduction by tying financial planning to cybersecurity goals. The results demonstrate how proactive, AI-driven investments outperform other options in reducing the likelihood of breaches while optimising ROI and maintaining business continuity.

Subject Classification: *68M25.*

Keywords: *Cybersecurity investment, Risk–return modelling, Optimization, Financial planning, Resilience.*

I. Introduction

The robustness of computer security frameworks has emerged as a critical component in today's interconnected organisational contexts for maintaining business continuity and protecting sensitive assets [1, 2]. Because networks are the foundation of financial systems, vital infrastructures, and commercial processes, security architectural flaws expose organisations to increasing risks from insider threats, cybercrime, and sophisticated persistent assaults [3, 4]. Even if they are helpful, traditional reactive methods are inadequate to counter the cunning and tenacity of contemporary opponents [5, 6]. Therefore, in order to foresee risks, bolster defences, and strike a balance between costs and quantifiable benefits in risk reduction, proactive investment techniques are needed. Investing in strategic security is not only a technological issue; it is also an organisational and financial one [7, 8, 9]. Businesses must decide how effectively to divide their limited funds among several security layers, including endpoint monitoring, encryption, intrusion detection, and incident response capabilities [10, 11].

[@] *E-mail:* **kanitha@maher.ac.in**

II. Mathematical and Computational Modeling

A. *Formulation of investment optimization problem*

Define total investment budget:

$$B \in \mathbb{R}^{+}$$

Investment decision vector:

$$x = (x^1, x^2, \dots, x_n), where\ x_i \geq 0 \tag{1}$$

Budget constraint:

$$\Sigma_i x_i \leq B$$

Breach probability function for control i:

$$P_i(x_i) = \alpha_i e^{-\beta_i x_i} \tag{2}$$

Aggregate breach probability:

$$P(x) = \prod_i P_i(x_i) \tag{3}$$

Expected residual loss with investment:

$$L(x) = L^0 \cdot P(x) \tag{4}$$

Risk reduction benefit:

$$R(x) = L^0 - L(x) \tag{5}$$

Investment cost:

$$C(x) = \Sigma_i x_i$$

Net utility function:

$$U(x) = R(x) - \lambda C(x), \tag{6}$$

Optimization objective:
Maximize U(x)
Subject to:

$$x_i \geq 0, \Sigma_i x_i \leq B$$

Gradient condition for optimality:

$$\frac{\partial U(x)}{\partial x_i} = 0$$

Solve for:

$$x* = (x^1 *, x^2 *, \dots, x_n *) \tag{7}$$

B. *Risk–return modeling for cybersecurity investments*

Below Figure 1 represents the Multicolor Framework of Risk–Return Modelling for Cybersecurity Investments.

Define investment vector:

$$x = (x^1, x^2, \dots, x_n)$$

Expected return from control i:

$$r_i = \frac{R_i(x_i)}{x_i} \tag{8}$$

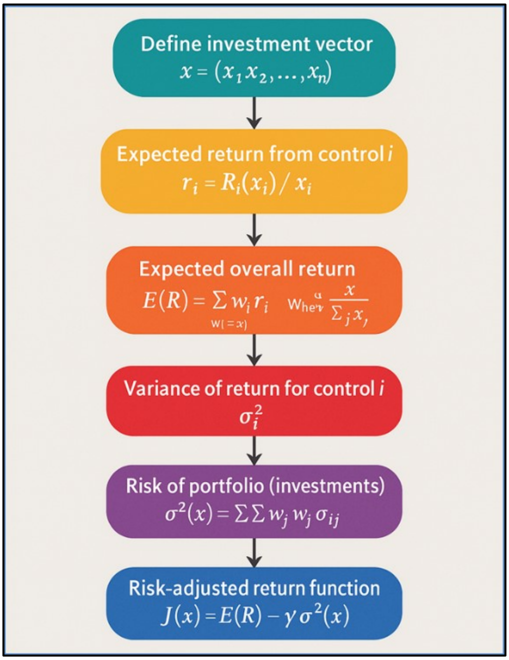

Figure 1
Multicolor Framework of Risk–Return Modeling for Cybersecurity Investments

Expected overall return:

$$E(R) = \Sigma_i w_i r_i$$

$$where\ w_i = \frac{x_i}{\Sigma_j x_j}$$

Risk of portfolio (investments):

$$\sigma^2(x) = \Sigma_i \Sigma_j w_i w_j \sigma_{ij} \tag{9}$$

Risk-adjusted return function:

$$J(x) = E(R) - \gamma \sigma^2(x) \tag{10}$$

where γ = risk aversion parameter

Constraint:

$$\Sigma_i w_i = 1$$

Positive allocation:

$$w_i \geq 0$$

Sharpe-like cybersecurity ratio:

$$S(x) = \frac{E(R)}{\sigma(x)} \tag{11}$$

Optimal allocation condition:

$$\frac{\partial J(x)}{\partial w_i} = 0$$

Solve for optimal weights:

$$w = (w^1 *, w^2 *, \dots, w_n *) \tag{12}$$

Derive optimal return:

$$E(R *) = \Sigma_i w_i * r_i \tag{13}$$

Optimal risk:

$$\sigma * = \sqrt{\Sigma_i \Sigma_j w_i * w_j * \sigma_{ij}} \tag{14}$$

III. Proposed Framework for Investment-Driven Security

A. *Architecture of strategic security investment model*

In order to maximise resilience and minimise vulnerabilities, the model creates a layered security architecture that aligns organisational assets, threat intelligence, and defence objectives with the best possible resource allocation.

Define total available investment:

$$B \in \mathbb{R}^+$$

Investment allocation vector:

$$(1) \quad y = (y^1, y^2, \dots, y_m), with\ y_j \geq 0$$

Budget constraint:

$$\Sigma_j y_j \leq B$$

Effectiveness of layer j:

$$E_j(y_j) = 1 - e^{-\theta_j y_j}, where\ \theta_j > 0 \tag{15}$$

Aggregate system effectiveness:

$$E(y) = 1 - \prod_j \left(1 - E_j(y_j)\right) \tag{16}$$

Breach probability after investment:

$$P(y) = 1 - E(y) \tag{17}$$

Residual loss with investment:

$$L(y) = L^0 \cdot P(y) \tag{18}$$

Benefit of investment:

$$B(y) = L^0 - L(y) \tag{19}$$

Cost of implementation:

$$C(y) = \Sigma_j y_j$$

Utility function:

$$U(y) = B(y) - \lambda C(y) \tag{20}$$

Optimization objective:

$$Maximize\ U(y)$$

Subject to:

$$y_j \geq 0, \Sigma_j y_j \leq B$$

Solution yields optimal allocation:

$$y* = (y^1*, y^2*, \ldots, y_m*) \tag{21}$$

B. *Integration of financial planning with cybersecurity defense layers*

By prioritising investments across several security levels and integrating cost-benefit analysis, financial planning ensures balanced expenditures while bolstering defences against changing threats and operational hazards.

Define investment allocation per layer:

$$y = (y^1, y^2, \ldots, y_m)$$

Define weight (financial proportion) per layer:

$$w_j = \frac{y_j}{\Sigma_k y_k} \tag{22}$$

Expected security return of layer j:

$$r_j = \frac{B_j(y_j)}{y_j} \tag{23}$$

Aggregate expected return:

$$E(R) = \Sigma_j w_j r_j \tag{24}$$

Portfolio risk across layers:

$$\sigma^2(y) = \Sigma_j \Sigma_k w_j w_k \sigma_{jk} \tag{25}$$

Risk-adjusted financial-security function:

$$J(y) = E(R) - \gamma \sigma^2(y) \tag{26}$$

Constraint:

$$\Sigma_j w_j = 1$$

Non-negativity:

$$w_j \geq 0$$

ROI for investment allocation:

$$ROI(y) = \frac{(B(y) - \Sigma_j y_j)}{\Sigma_j y_j} \tag{27}$$

Sharpe-like cybersecurity ratio:

$$S(y) = \frac{E(R)}{\sigma(y)} \tag{28}$$

Solution yields optimal allocation:

$$y* = \arg\max J(y) \tag{29}$$

IV. Result and Discussion

With an annual investment of \$0.8M, reactive tactics still face a high breach chance of 36.2%, according to the data, which also shows that they only achieve a 25.7% return on investment and a 21.4% loss reduction (shows in Figure 2).

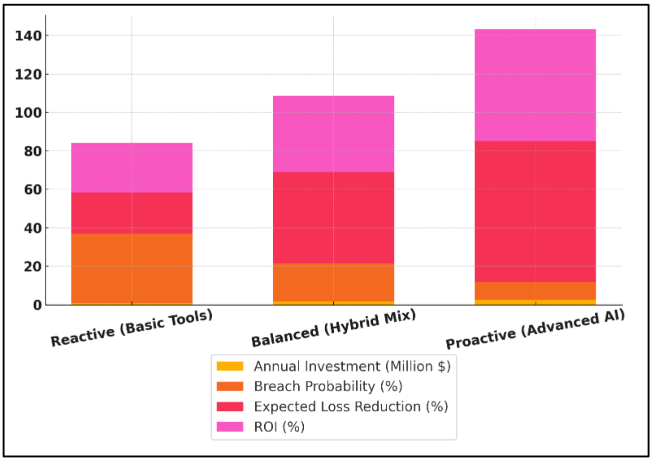

Figure 2
Comparative Performance of Cybersecurity Investment Strategies

The risk of a breach is reduced to 19.7% with balanced solutions, which need a $1.6 million investment. The predicted loss reduction is 47.8%, and the return on investment is 39.5% (shows in Figure 3).

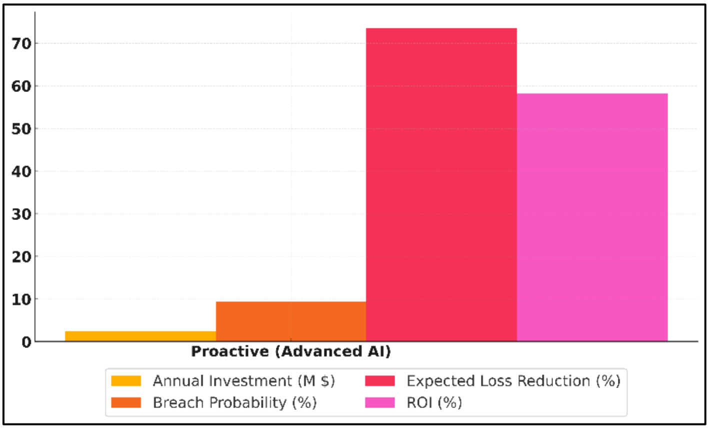

Figure 3
Performance Metrics of Proactive Cybersecurity Strategy

Although proactive techniques are more expensive ($2.4M), they perform the best, lowering the breach probability to 9.3%, cutting losses by 73.5%.

V. Conclusion

Building robust organisational networks that can survive changing digital threats requires strategic investment in cybersecurity. Organisations may efficiently distribute resources across layered defences, balancing costs with quantifiable risk reductions, by defining security as a technological and financial priority. In order to make sure that security investments are proactive, sustainable, and strategically aligned with organisational goals, the suggested framework emphasises the integration of financial planning and optimisation modelling. This eventually promotes long-term resilience, operational continuity, and stakeholder trust.

References

[1] N. Dragoni, A. L. Lafuente, F. Massacci, and A. Schlichtkrull, "Are we preparing students to build security in? A survey of European cybersecurity in higher education programs," *IEEE Security & Privacy*, vol. 19, no. 1, pp. 81–88 (2021).

[2] T. Balon and I. Baggili, "Cybercompetitions: A survey of competitions, tools, and systems to support cybersecurity education," *Education and Information Technologies,* vol. 28, pp. 11759–11791 (2023).

[3] T. M. Fernández-Caramés and P. Fraga-Lamas, "Use case based blended teaching of IIoT cybersecurity in the Industry 4.0 era," *Applied Sciences*, vol. 10, no. 16, pp. 5607 (2020).

[4] R. N. Wadibhasme, A. U. Chaudhari, P. Khobragade, H. D. Mehta, R. Agrawal, and C. Dhule, "Detection and prevention of malicious activities in vulnerable network security using deep learning," in *Proc. 2024 Int. Conf. Innovations and Challenges in Emerging Technologies* (ICICET), pp. 1–6 (2024).

[5] T. Branoff, J. Mohammed, and J. Brown, "The role of spatial visualization ability in course outcomes and student retention within technology programs," *Journal for Geometry and Graphics*, vol. 26, no. 2, pp. 159–170 (2022).

[6] F. Mizrak, "Integrating cybersecurity risk management into strategic management: A comprehensive literature review," *Research Journal of Business Management,* vol. 10, no. 2, pp. 98–108 (2023).

[7] J. Kotsias, A. Ahmad, and R. Scheepers, "Adopting and integrating cyber-threat intelligence in a commercial organisation," *European Journal of Information Systems*, vol. 32, no. 1, pp. 35–51 (2023).

[8] S. N. Ajani, J. Moulick, J. Mohur, R. H. J. Rani, A. D. Sonawane, and P. Shende, "Enhancing secure access in RF communications through advanced elliptic curve encryption," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 29, no. 2-A, pp. 571–579 (2026), doi: 10.47974/JDMSC-2498.

[9] S. Harsha, K. Aswini, G. Sahith, G. V. N. Abhiram, and D. B. Kumar, "Data integrity verification in images through SHA-based security," *International Journal of Advanced Computer Engineering and Communication Technology* (IJACECT), vol. 14, no. 1, pp. 75–84 (Apr. 2025).

[10] A. K. Rajpoot, D. Dhabliya, V. N. Trupti, T. A. Wani, K. Gupta, and L. Lakshmanan, "Quantum cryptography: Assessing the security and practicality of quantum key distribution in modern communication networks," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 29, no. 2-B, pp. 979–986 (2026), doi: 10.47974/JDMSC-2549.

[11] V. D. Joshi, M. Sharma, R. K. Alhefthi, and M. Purohit, "Optimal route planning for multi-level multi-choice transportation problem with uncertain parameters using Lagrange's interpolating polynomial," *Journal of Information and Optimization Sciences*, vol. 46, no. 3, pp. 761–766 (2025), doi: 10.47974/JIOS-1794.

Received April, 2025