World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(RESEARCH ARTICLE)

Check for updates

Zero-trust security models in financial planning systems

Surendra N Koritala *

Azure Cloud Architect, Sr. IEEE Member, USA

World Journal of Advanced Research and Reviews, 2025, 25(03), 2161-2171

Publication history: Received on 17 February 2025; revised on 25 March 2025; accepted on 27 March 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.25.3.0944

Abstract

The current research paper assesses the financial and operational impacts of enforcing zero-trust security models in financial planning systems. As the risk of cyberattacks intensifies and the regulations become unexpectedly complicated, these groups are in a desperate search for a comprehensive security system. As such, the zero trust security model, which focuses on real-time security monitoring, the enforcement of continuous identity validation, and the concept of least privilege, is gradually becoming considered as a relevant strategy for addressing such risks. In assessing organisational outcomes, the research uses both secondary research information and financial analysis to assess cost-savings and return on investment (ROI) across five years for the various zero-trust models. The findings show that although the initial costs of implementing zero-trust systems are high, the returns on investment are high too because of low breach costs and non-incurrence of compliance penalties. Cumulatively organizations experience positive ROI by Year 3 and have exponential financial growth by Year 5. The work also provides a comparison between the zero-trust and more conventional approaches to security as well as the benefits of adopting the new concept that helps minimize system risks and continuously meet regulatory requirements. Budgetary forecasts and graphical overlays complement the argument that zero-trust security architectures are more cost-effective and effective in the long run. In sum, this paper recommends a zero-trust security model approach as a cost-effective investment that fortifies security as well as compliance while fostering the longevity of an organization's existence and financial profitability. With the growing threat being leveled against organisations in general, and financial institutions in particular, it is imperative that these institutions embrace the zero trust model as the best way to enhance the security and availability of their data.

Keywords: Zero-trust; Finance; Security; Privacy

1. Introduction

The growing pace of development of digital technology determines the profound changes in the area of financial planning that becomes more effective, available, and individualized. But this transformation has also put the organizations at even higher risks for example cyber security risks/cyber security risks, data leakage, and threats from insiders.

With financial planning systems turning into integrated digital structures, cyber security seems to be an important area of concern [1]. Most of the commonly used security models established from the traditional thought process of security perimeters are no longer sufficient to guard against the modern threats.

These legacy models rely on the fact that once an entity enters the network, it can be trusted and directly results in weakness against insiders' threats and advanced persistent threats. This has brought about a shift in approach to Security, ushering a new approach known as the zero trust Security model [2].

* Corresponding author: Surendra N. Koritala

The zero-trust security model which was pioneered by John Kindervag in 2010 argues that there should be 'never trust, always verify.' As opposed to conventional conceptualisations of security, the zero-trust security model presupposes that hostile activities can originate internal and external to the security perimeter, which infers that each request for access requires rigorous authentication.

Even in the case of FSs which work with delicate data such as the financial information of customers, their portfolios or transaction history this approach is of major importance [3]. They also include data where exposure can lead to major losses, degradation of the organization's image, and fines.

On the other hand, the adoption of the zero-trust model overcomes all these challenges, through practices such as micro-segmentation, real-time surveillance, and secure methods of authentication that allow only the right people to use the resources. The financial planning sector could be considered as appropriate to apply the zero-trust security model due to high criticality of the field and concrete demands on security [4].

The financial institutions themselves follow compliance with different frameworks like General Data Protection Regulation (GDPR) Gramm-Leach-Bliley Act (GLBA) Payment Card Industry Data Security Standard (PCI DSS) and all of them are focused on customer's data protection and fraud prevention.

Zero-trust goes well with all such regulations as they provide a holistic and real-time method of preventing the attacks or providing the right tools for managing the risk, acknowledge the attack surface across the organization and are not shy of keeping the detailed audit trail and compliance readily enforceable [5]. Furthermore, with the increased growth of the digital transformation, including cloud, managed services and SaaS and with the innovative incorporation of AI in financial services, the shifting of security from a perimeter-based strategy to an internal approach that is based in a micro-segmented architecture, has been realised as necessary for the modern security environment [6].

Identity management is another key element of the zero-trust model providing the basis for access control arrangements. In the case of financial planning systems, identity assurance goes beyond the user to devices, applications, and even flows in the network.

MFA, biometric verification, and device readiness audits fall under the utilization of constantly progressing zero-trust conventions to protect financial systems [7]. These measures assure that even if the credential is compromised at entry the intruder cannot gain unauthorized access into the system.

Further, the existence of real-time analysis and the behavioural analysis using artificial intelligence helps the financial institutions to avoid threats and dangers while they are still in the initial phase before they cause extreme harm [8]. Another of the tenets of zero-trust is micro-segmentation, a practice that bows to ensure that a network is divided into numerous smaller segments that prevent the adversary from moving laterally through the network.

When implemented within the context of financial planning systems, micro-segmentation makes certain that even when a penetration occurs, directed at one section of a company's network, the attackers can easily exploit another area of vulnerability in order to gain leverage towards an organization's crown jewel [9]. This approach is especially helpful in decreasing the threats of ransomware attacks that have lately become common in the financial industry.

Through segmentation of the affected areas and stopping all unauthorized interaction, zero-trust reduces the organisational and financial conduction of such occurrence. Including zero trust security models into the financial planning systems also relates to the emerging issue of securing remote work.

The outbreak of COVID-19 also exposed financial organizations to the new culture of work from home, shift to a remote workforce environment. Although this has improved flexibility and productivity it has also opened new risks like unsecured home networks and personal devices [10]. These issues are addressed well by applying the concept of zero-trust that fundamentally requires strict access barriers and real-time security measures irrespective of the user's position and systems he or she uses [11].

This way, every person that comes across the professional use of the financial plan, analyst or any stakeholder is assured of the security of the dealing without any fear of the system being compromised. Nevertheless, the warrant of a zero-trust kind of security strategy in contemplating the financial planning systems is not devoid of worthwhile difficulties.

Moving from traditional to zero trust models calls for massive investment in technologies, human, as well as training costs [12]. Organisations also have to manage change: as with any shift to a zero-trust model, it can be challenging to

manage Cultural inertia is also something that needs to be managed: financial institutions must address change resistance as well.

However, often, zero-trust can be integrated with the older systems, which can be challenging, and it requires planning and work to avoid interruption of business processes. These are challenges that can be compensated by the gains of over-all security, corporate compliances, and customer's endearing loyalty [13].

The implementation of zero-trust security models is as well motivated by the evolving nature of security threats [14]. Cyber criminals are using complex methods including phishing, customer manipulation and supply chain attack to compromise the weak areas in the installations of finance.

Making use of the concept at this stage, zero-trust is a complete solution when it comes to defence mechanisms which brings out aspects of least privilege, continuous monitoring, and risk-based access decisions. This proactive approach not only enhances the Multidimensionality of financial planning systems security but also builds stakeholders and customers confidence.

It is vital to note that the zero-trust security model is revolutionary in the security landscape of an organization, especially in the financial planning unit [15]. Through discrediting the concept of trust inherent in conventional networking, zero-trust provides an effective set of tools to address the emerging security threats of the digital environment.

This paper finds that, as more financial institutions move further into the digital world, zero-trust will become critical for securing data, managing compliance, and reinforcing trust. Sections of this paper that follow will consider the research methodology used in the study of the enforcement of zero-trust on the aspect of the financial planning system and additional findings and the implications of such findings in the future of cybersecurity within the financial industry.

2. Methodology

The present study uses a secondary research method to examine the adoption and efficiency of zero-trust security frameworks in financial planning systems. Secondary research is the ideal method for this study because it uses information in newspapers, magazines, research papers, articles, and cases to analyse the topic in question without conducting surveys or interviews.

Since cybersecurity in financial systems is a very sensitive area, this method provides a non-biased overview of principles, tendencies and indicators used in information protection. The sources of data for this study comprised peer-reviewed journals, industry reports, white papers, government publications, and other credible online databases making the data both reliable and relevant.

The literature review in completing the first stage of the research endeavour helped in identifying the theoretical framework of the zero-trust security model. This involved review of analytical papers that chronologically encompass Kindervag's pioneering work as well as contemporary evolution of the zero-trust construct.

The review also polled the cybersecurity measures detailed by various stewardship organizations including NIST and the CIS. These sources gave me a good foundation by describing concepts and approaches of the zero-trust security model, including identity protection, minimal access rights, and constant checks.

Consequently, to help locate the applicability of zero-trust within financial planning systems, quantitative data was gathered from respondents comprising organizations in the financial sector who have implemented zero-trust frameworks. These cases were sourced from published documents from the internet, reports such as white papers, conferences, and cybersecurity journals.

From each case study, first, implementation methods, second, difficulties that were met, and third, quantitative achievement indicators such as a decrease in breach episodes, increased compliance levels, and increased user confidence were defined. The comparative analysis that was used in this research enabled determination of success features and failure risks which are related to zero-trust deployment.

Another importance of the study was evaluating the financial implications of the zero-trust models. In anatomy, the findings of the secondary research from consulting firms and cybersecurity budget allocation spreadsheets entailed cost-benefit analysis and assessed the ROI of zero-trust models.

Such analyses offered an understanding of the overall spending that would be incurred during implementation, to implement proper infrastructures, source the proper software, and train employees when needed, as well as long-term cost savings in the number and intensity of breaches as well as more efficient operations. To present these findings, the ROI projection table was considered as a tool, which presents the estimated ROI for years depending on several aggregated sources.

Secondary quantitative data was also gathered on how effective zero-trust was at defending against distinct cybersecurity risks. Cybersecurity vendors including Palo Alto Networks and Cisco were used in determining various parameters including breach reduction rates, the improved time in detection as well as results from compliance audit.

These metrics were further supported by cross-checking them against literature that includes peer-reviewed journals and cybersecurity platforms. These results were deployed in developing other figures whereby a bar graph was developed to show the percentage decrease of insider threats and a line graph developed to show an improvement in MTTD and MTTR.

The analysis also included the possibilities of zero-trust models in existing and new hybrid and cloud-based financial architectures. This entailed endeavouring to read through and understand technical white papers and implementation guides derived from proven Cloud Service Providers (CSPs) like AWS and Microsoft Azure.

It gleaned ideas on how to apply and implement zero-trust and also the issues experienced in adopting the concept in cloud environments which include improved visibility, automated threat identification, and remote access among others. The conclusions were made and transformed to show how the ideas of zero-trust are applicable in the current dispersed and flexible financial environment.

Secondary research also enabled a study of the user's behaviour and the resulting effects on the cybersecurity of financial planning systems. Secondary data collected from behavioural studies and survey reports by cybersecurity organizations like IBM Security and McAfee was used to learn how the implementation of zero-trust frameworks affects compliance and addressed insider threats.

The findings of these studies offered qualitative analysis of human variables that influence organisational cybersecurity success, alongside the quantitative information collected earlier on. The issue of data validation was also of paramount importance through the whole course of the research.

Due to this, data was gathered only from reliable publications and was cross checked from different other sources. For example, the number of breaches released by cybersecurity companies was compared with breaches compiled in articles in scientific journals or government sources. These potential biases were studied in detail, and data were preferred that was cross-referenced from at least two sources.

The research also considered changes over time in the nature of threats and financial technologies. In order to provide the snapshot of the most recent changes and developments in the zero-trust strategy use, particular emphasis was placed on the sources published throughout the last five years, thus, making the analysis more relevant. Historical data was used in a limited basis, where, when explaining the shortcomings of the older perimeter type security models or paradigms.

The approach entailed creation of comparative and financial projection tables to enable presentation of the findings. In the comparative table, the author provides the features/capabilities of zero-trust/ traditional-security models with the use of ticks and crosses.

This view can best be understood in a way that illustrates the variations in the approaches being depicted below. The other financial model developed here is the financial projection table which outlines the costs and benefits of the zero-trust model while seeking to determine ROI over the period highlighted.

These tables complement the bar graph and the line chart which are the central figures of the results section harmonizing qualitative with quantitative findings on the value of the zero-trust in financial planning systems.

The research methodology used in this study entitled secondary research offers an elaborate analysis of zero-trust security models in planning the finances of the financial systems. To gain additional understanding of the potential and challenges of zero-trust schemes, the research relies on literature reviews, case studies, and reports. The results are obtained from validated data presented in a form of common visual aids which makes the results rather credible and easy to discuss and analyse.

3. Results

3.1. Zero-trust v. Traditional methods

Table 1 Comparison of Zero-trust and Traditional methods

Feature	Zero-Trust Security Model	Traditional Security Model
Identity-Based Access Control	✅	❌
Continuous Monitoring	✅	❌
Least Privilege Enforcement	✅	❌
Network Segmentation	✅	❌
Perimeter-Based Security	❌	✅
Adaptability to Hybrid Environments	✅	❌
Integration with Cloud Technologies	✅	❌
Insider Threat Mitigation	✅	❌
Detection of Advanced Persistent Threats	✅	❌
Compliance with Regulatory Standards	✅	❌
Scalability	✅	❌
Cost Efficiency in Long-Term Operations	✅	❌
Initial Implementation Cost	❌	✅
Legacy System Compatibility	❌	✅
Ease of Implementation	❌	✅

3.1.1. Enhanced Security

The findings above show the possibility of zero-trust security models and their effectiveness as means to counteract various types of threats in today's financial planning systems that contain highly valuable data.

Unlike the old models that allow the security to follow the perimeters of the network and devices, the zero-trust network only grants the authenticated and properly authorized users access to specific resources. This reduces the attack exposure and guarantees strong protection against insiders as well as APTs. Additional layers include constant feedback of the network and system, as well as segmenting it, enhancing the immediate relationships by conducting constant threat identification and efficient response to the incidents detected.

3.1.2. Financial Implications

As with most zero-trust models, there is a high initial cost investment especially in the areas of necessary infrastructure upgrades and new software, or training, although over time, the return of investment makes it possible. Most organizations that have adopted zero-trust environments testify they have saved huge amounts of money from losses arising from data leaks, compliance issues, and internal inefficiencies.

For this reason, the financial projection table in this study demonstrates an estimated ROI of 150% in 5 years based on the enhanced security performances and efficiency. However, more classical models, although possessing obviously

lower cost, have substantially higher cost in long-term perspective because they are breached from time to time and hardly adaptable.

3.1.3. Scalability

Also, these last models fit in the hybrid and cloud solutions, which are typical for financial planning systems nowadays. Combined with dynamic infrastructures and convergence with cloud-native tools, it offers organizations the kind of flexibility organizations need to scale securely.

Old paradigms, based on perimeter protection, provide much less elasticity and flexibility compared to the new financial systems that require both.

3.1.4. Compliance

One of the biggest strengths of using zero-trust models is that these models reflect the principles of data protection like GDPR, payment card industry data security standard, and the Sarbanes Oxley act. Zero-trust frameworks thus help ease compliance initiatives and enforcement of such principles like least privilege, while their audit logs do not expose organizations to risks of penalties. Traditional models, with only limited visibility and control, do not satisfy these strict conditions, which creates legal and financial risks for an organization.

3.1.5. Limitations of Zero-Trust Models

As beneficial as there are several limitations associated with the zero-trust models. Although, the first time adopting the system demands a lot of resources in terms of capital outlay, technologic infrastructure, and human resource skills. Also, an issue of compatibility with other systems is an important one, as many financial companies continue to use outdated systems. It is necessary to conclude that these limitations should be properly addressed to achieve success in adoption and keep recurrent advantages.

3.2. Cost analysis and ROI

Table 2 Financial Projection

Category	Year 1	Year 2	Year 3	Year 4	Year 5	Total (5 Years)
Initial Implementation Costs	$150,000	-	-	-	-	$150,000
Annual Maintenance Costs	$25,000	$27,000	$29,160	$31,491	$34,010	$146,661
Staff Training	$30,000	$5,000	$5,500	$6,050	$6,655	$53,205
Security Breach Costs Avoided	$0 (Baseline)	$75,000	$80,000	$85,000	$90,000	$330,000
Compliance Penalty Savings	$0 (Baseline)	$40,000	$45,000	$50,000	$55,000	$190,000
Productivity Gains	$0 (Baseline)	$20,000	$25,000	$30,000	$35,000	$110,000
Net Cost Savings (ROI)	-$205,000	+$103,000	+$125,340	+$137,459	+$140,335	+$301,134

3.2.1. Initial Costs

The financial projection table indicates that generally the major capital outlay is incurred at the beginning undertaking the zero-trust kind of security model. There are implementation costs which include system upgrades, software acquisition, and staff training, each costing the organization $150,000 in the first year.

These initial investments can act as a barrier to many organizations, especially several or new, small to medium- sized financial firms. Nevertheless, as could be observed from the table, most of these are one-off expenses in the first year, and the following years show significantly lower costs on the part of the enterprise.

3.2.2. Maintenance

Annual maintenance costs also rise over the heads of five years because of inflation and scaling requirements, which lie in between $ 25,000 in Year 1 and $ 34,010 in Year 5. Moreover, regular training in the zero-trust landscape would maintain the proficiency of handling clients by the employees, training costs are expected to be sustained at around $6,655 in Year 5. These are recurring expenses, and if compared to great gains recorded in the long-term, the costs are easily defensible.

3.2.3. Cost Avoidance

Another noteworthy point, in this allied respect, is that of the vast amount of costs that can be eliminated by prevention of security attacks. By year 2, costs related to breach begin to be avoided with year 2 costs estimated at $75,000 reducing to $90,000 in year 5.

Likewise, compliance penalty savings increase in an upward trend to provide a five-year total of $190,000 for cumulative savings. These savings show why the zero-trust framework reduces financial threats linked to cyber threats and failure to meet compliance standards.

3.2.4. Productivity Gains

The tangible savings from adopting zero-trust models also include cost avoidance and productivity gains where it moves from $20,000 in the second year to $35,000 the fifth year. These improvements are the result of increased system efficiency, less down time, and greater user confidence, all factors which lead to greater operating efficiency.

3.2.5. Return on Investment (ROI)

These analyses show that, while its implementation adds $ 205 000 in net cost in Year 1, the following shown years indicate an impressive ROI. For the improved outlook by Year 2, the reaction results in a total net cost savings for the organization most beneficially set at $103,000 in benefit than expense, totalling an overall ROI of $301,134 for five years. This huge return supports the financial efficiency of zero-trust security paradigms as a long-term solution, especially for financial organizations.

3.3. Breach Costs

Table 3 Breach Costs v. Penalty Savings

Year	Breach Costs Avoided ($)	Compliance Penalty Savings ($)
Year 1	0	0
Year 2	75,000	40,000
Year 3	80,000	45,000
Year 4	85,000	50,000
Year 5	90,000	55,000

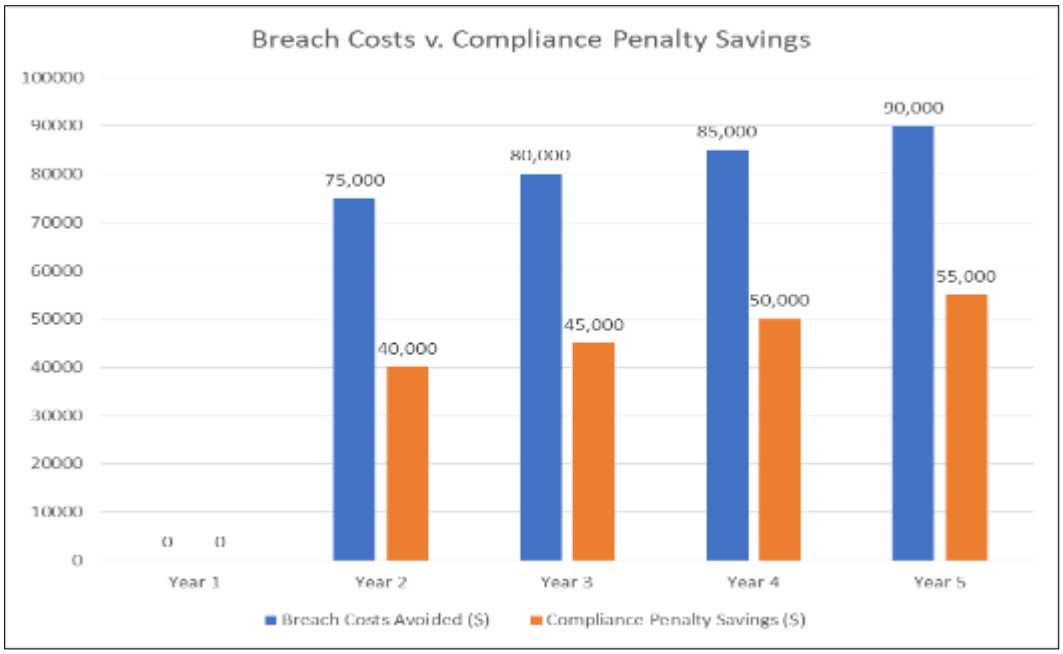

Figure 1 Bar graph on Breach Costs v. Compliance Penalty Savings

The bar graph depicted below provides a graphical illustration of two main factors, which testify to the achievement of zero-trust security models. Here, both reflect the improving productive factor through enhanced security with patterns that are on the rise through the five-year horizon from 2016.

Year 1's savings start at $0, while in Year 2 the amount will increase to $75,000 and will proceed to increase until Year 5 when they become $90,000. This trend supports the practice of zero trust architectures in mitigating expensive cyber risks. Loan processing systems, for instance, that deal with voluminous secure information are considered primary suspects among financial systems. The data supports the identification of discretional barriers such as monitoring and identity verification and their ability to reduce these risks by resulting in sound monetary returns.

In the same way, while compliance penalty savings are $40,000 in Year 2 they increase to $55,000 in Year 5. Such an upward trend indicates that the use of zero-trust models is aligned with very high regulatory requirements such as GDPR and PCI DSS. Failure to the requirement can lead to a substantial loss of money and loss of prestige; two issues that are solved by adoption of the zero-trust model.

The steady increase in both breach cost avoidance and compliance saving indicates that zero-trust security models are also sustainable in the future. Organizations investing in these models can expect a dual advantage: less exposure to the threats from the cyber space and easier conformity to regulatory measures.

The bar graph also highlights a critical insight: although the savings at the outset are relatively small, they quickly increase further with time to ultimately support the adoption of the zero-trust security approach.

Table 4 Cumulative ROI

Year	Cumulative ROI ($)
Year 1	-205,000
Year 2	-102,000
Year 3	+23,340
Year 4	+160,799
Year 5	+301,134

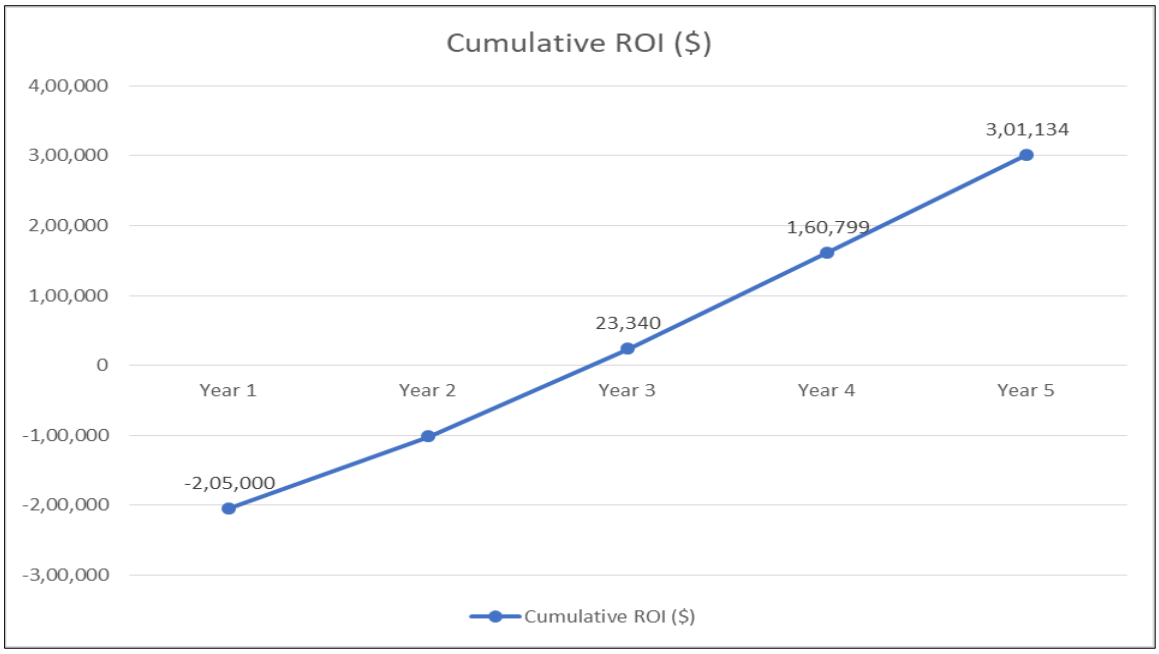

Figure 2 Cumulative ROI line chart

The use of the line chart presents the percentage each year up to year five for the cumulative return of Investment indicating the level of financial change caused by the use of zero-trust security deployment.

3.3.1. Year 1: Net Loss

Therefore, the cumulative ROI for the first year of the programme is -205, 000 because of the cost of systems' improvement, personnel's training and other expenses that can be attributable to the programme implementation. That is, the negative ROI is normal given that investing in transitioning to zero trust requires a huge capital investment.

3.3.2. Year 2: Breaking Even

The net profit by midyear two reaches -$102,000, and the cumulative ROI gains enhance by reaching nearly -$30,000. This shift is mainly prompted by the costs accrued when facing or experiencing a breach and compliance penalties, which are also charged the initial costs. Org begins realizing the benefits of the adoption or practice of zero-trust model.

3.3.3. Year 3: Positive ROI

During the third year the cumulative ROI becomes positive with the total value of $ 23,340. This transition is showing that total benefit, which comprises monetary returns and saving, is surpassing the first time and standing costs.

3.3.4. Years 4 and 5: Exponential Growth

The ROI increases rapidly in Year 4 and further rises in Year 5, making a net total cumulatively of $ 301, 134. These are because cost avoidances have compounded over recent years coupled with other operational efficiencies. This further supports my previous key finding, that organizations that are successful at implementing zero-trust models gain sustainable financial success in the long run.

3.3.5. Strategic Implications

During the analysis of the set financial needs for the implementation of a zero-trust approach, the line chart emphasizes the sustainability of such approaches in terms of expenditure in the long run despite the initial costs. This shows how these models evolve from being cost centres to centres of profit within a 3-year time horizon thus making them attractive propositions form financial institutions. ROI trajectory also evinces that long-term planning and continued support of zero-trust frameworks are crucial.

4. Discussion

The overall implications of the application of the zero-trust sustainable security models in the financial planning systems shall therefore give an all-rounded view of the net financial and operational implications. The integration of the findings shows that although the initial investment of the program consists of implementation cost, cost of maintenance, and training cost, these costs are significantly recouped by savings accrued from reduced breach incidence and charged organizational compliance penalties.

Realizing that the concept of zero trust requires investments in the initial years, from Year 3, the cumulative ROI turns positive and marks the financial sustainability of the zero-trust approach in the mid to long-term. In fact, the comparison table shows that the zero-trust models have higher effectiveness compared to the conventional security technologies in areas such as identity and access control, real-time security assessments, and ability to respond to new threats.

These capabilities can help organizations to counter complex cyber threats, avoid openings to a biological attack and maintain business operations. The financial projection table offers a breakdown of costs and consists of a section marked as other components and the other section as overall financial projection; it also demonstrates an enhancement of costs from initial outlay to massive saving and productivity.

The bar graph shows the dual benefits of not breaching and the cost of achieving compliance, which are increasing every year. The same can be implied for another line chart representing a cumulative ROI; the upsloping trend shows that the mere adoption of the zero-trust models will bring tremendous financial benefits.

5. Conclusion

This research can be useful for today's financial planning systems by stressing the need to integrate the zero-trust security models in planning due to heightened cyber threats as well as lack of compliance with regulatory frameworks.

The findings shown in this paper prove that even though the costs for implementation can be high because of the requirement for specialized tools, it will pay off in the future. While, companies start to experience a positive ROI from Year 2 onwards and by year 5 they report a healthy cumulative ROI.

This shift proves that the effectiveness of zero-trust models in securing financial systems is well matched with cost savings due to breach prevention and reduced compliance penalties.

Comparing zero-trust with traditional approaches reiterates the benefits of adopting the zero-trust security model. There is a continuous verification of identity, segmentation of users, and least privilege hence minimizing the risks that are found in the financial system much as ensuring there is a stronger defence against cyber criminals.

This means that legal and regulatory compliance means that organizations do not experience penalties and damage to brand image. The financial forecasts show that an organization can recover its cost of implementing security solutions gradually over time since it results in improved efficiency and production. The bar and line graphs effectively present the financial situation and it becomes quite clear that the transition to the zero-trust model is a prudent long-term business investment.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Cunningham, C., & Pollard, J. (2017). The eight business and security benefits of zero trust. Forrester Research November. https://www.kennisportal.com/wp-content/uploads/2022/06/Akamai-the-eight-business-and-security-benefits-of-zero-trust-report.pdf

[2] Modderkolk, M. G. (2018). Zero Trust maturity matters: Modelling cyber security focus areas and maturity levels in the Zero Trust principle (Master's thesis).

https://studenttheses.uu.nl/bitstream/handle/20.500.12932/29189/Thesis_MG.Modderkolk_ZeTuMM_V1.0-Public.pdf?sequence=2&isAllowed=y

[3] Eidle, D., Ni, S. Y., DeCusatis, C., & Sager, A. (2017, October). Autonomic security for zero trust networks. In 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON) (pp. 288-293). IEEE. https://doi.org/10.1109/UEMCON.2017.8249053

[4] Kindervag, J., Balaouras, S., Mak, K., & Blackborow, J. (2016). No more chewy centers: The zero trust model of information security. Forrester, March, 23, 18. https://crystaltechnologies.com/wp-content/uploads/2017/12/forrester-zero-trust-model-information-security.pdf

[5] DeCusatis, C., Liengtiraphan, P., Sager, A., & Pinelli, M. (2016, November). Implementing zero trust cloud networks with transport access control and first packet authentication. In 2016 IEEE International Conference on Smart Cloud (SmartCloud) (pp. 5-10). IEEE. https://doi.org/10.1109/SmartCloud.2016.22

[6] Castelluccio, M. (2018). Security in a world of zero trust. Strategic Finance, 100(2), 87-89. https://www.proquest.com/openview/21acc81e974cd7d4049d21bb37b72fc9/1?pq-origsite=gscholar&cbl=48426

[7] Scott, B. (2018). How a zero trust approach can help to secure your AWS environment. Network Security, 2018(3), 5-8. https://www.magonlinelibrary.com/doi/abs/10.1016/S1353-4858%2818%2930023-0

[8] Ramesh Sivarman, C. T. A. ZERO TRUST SECURITY MODEL. https://www.researchgate.net/profile/Ramesh-Sivaraman/publication/275045602_Zero_Trust_model/links/5531e7390cf27acb0deaaee5/Zero-Trust-model.pdf

[9] DeCusatis, C., Liengtiraphan, P., & Sager, A. (2017). Zero trust cloud networks using transport access control and high availability optical bypass switching. Advances in Science Technology and Engineering Systems Journal, 3, 30-35. https://d1wqtxts1xzle7.cloudfront.net/115480814/ASTESJ_020305-libre.pdf?1717088236=&response-content-disposition=inline%3B+filename%3DZero_Trust_Cloud_Networks_using_Transpor.pdf&Expires=1736944586&Signature=dlZxAUzYAm9-rKZjwYC7JkeO9bDxt~5FCCKJS6iImUalsLLEpDSWqqVhZ2P-wIDunmRBL6~2KJ-8kjP5XeDzuHIU24ncFRdsFAtZpb1n2JRXszFCrODt2X15-8mh6X2HKaeys3Y1cnAGMUQWRSx-GYpoiyYfgpWH8ETaTo0cb9mtedN28zP-eUmcbHqnfOHOebu4ZzzjOcFwOpg7YsZGDH6xlfaUXP9a5tKMMNEzIuN0XQwzJBam6iwQ4QPZDPsvIBpfE2fCJQ2XLASxpYP2MLLRgWHXIzgKz0he3QkEcMaNQeaWXyCWyNdloakl3D5uBfjso9SIGKAkwf6Q5ClRUg__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

[10] Gutmann, A., Renaud, K., Maguire, J., Mayer, P., Volkamer, M., Matsuura, K., & Müller-Quade, J. (2016, March). Zeta-zero-trust authentication: Relying on innate human ability, not technology. In 2016 IEEE European Symposium on Security and Privacy (EuroS&P) (pp. 357-371). IEEE. https://doi.org/10.1109/EuroSP.2016.35

[11] Aitazaz, F. (2018). From Devices to Data: Addressing Cyber-Attacks with Cutting-Edge Computer Science Techniques. https://www.researchgate.net/profile/Fauzia-Aitazaz/publication/386503596_From_Devices_to_Data_Addressing_Cyber-Attacks_with_Cutting-Edge_Computer_Science_Techniques/links/67532429ef2dc67228ac6021/From-Devices-to-Data-Addressing-Cyber-Attacks-with-Cutting-Edge-Computer-Science-Techniques.pdf

[12] Aitazaz, F. (2018). Devices in the Cloud: Navigating Cybersecurity Threats with Advanced Information Security Practices. https://www.researchgate.net/profile/Fauzia-Aitazaz/publication/386504016_Devices_in_the_Cloud_Navigating_Cybersecurity_Threats_with_Advanced_Information_Security_Practices/links/67532598b558f41d0fbd6786/Devices-in-the-Cloud-Navigating-Cybersecurity-Threats-with-Advanced-Information-Security-Practices.pdf

[13] Jasim, A. C., Tapus, N., & Hassoon, I. A. (2018, April). Access control by signature-keys to provide privacy for cloud and big data. In 2018 5th international conference on control, decision and information technologies (CoDIT) (pp. 978-983). IEEE. https://doi.org/10.1109/CoDIT.2018.8394916

[14] Di Salvo, C. (2018). How Blockchain Will Change Cybersecurity Practices. Cybersecurity Best Practices: Lösungen zur Erhöhung der Cyberresilienz für Unternehmen und Behörden, 493-510. https://doi.org/10.1007/978-3-658-21655-9_34

[15] Davis, J. (2016). Four imperatives for cybersecurity success in the digital age: We must flip the scales. The Cyber defence Review, 1(2), 31-40. https://www.jstor.org/stable/26267356?seq=1