

Research Paper Summary

Title and Citation of the Paper

Title: Zero trust cybersecurity: Critical success factors and A maturity assessment framework

Authors: William Yeoh, Marina Liu, Malcolm Shore and Frank Jiang

Year of Publication: 2023

Citation:

W. Yeoh, M. Liu, M. Shore, and F. Jiang, "Zero trust cybersecurity: Critical success factors and a maturity assessment framework," *Computers & Security*, vol. 133, p. 103412, 2023. doi:

10.1016/j.cose.2023.103412

Objective and Research

- What is the main objective of the paper?
 - The main objective of the baseline paper by Yeoh and colleagues (2023) was to design a maturity model that organizations can use to check how much they are prepared for Zero Trust adoption. For Simplicity, they wanted to answer: "What makes Zero Trust successful, and how can we measure it in a way that actually helps organizations?"
- What research questions does the paper aim to address?
 - From the baseline paper (Yeoh et al., 2023):
 1. What are the critical success factors (CSFs) for adopting Zero Trust?
 2. How can these CSFs be structured into a practical framework that organizations can use to measure readiness?

Technique and Methodology

- What technique or methodology is proposed or used in the paper?
 - The method employed by Yeoh et al. (2023) was the Delphi, implying access to expert opinion as a result of a series of interviews to determine and ratify 43 Critical Success Factors (CSFs) by means of 8 dimensions. This method involves not only the technical controls, but also the elements of organizations and culture components in order to develop a practical, real life Zero Trust framework.
- How does this technique contribute to the field? Is it a novel approach or an improvement over existing methods?
 - In short, the technique is valuable because it provides them with a practical structured framework to evaluate the maturity of Zero Trust in the technical, organizational and cultural levels. The only difference is that it combines knowledge and skills of the expert with a multidimensional and detailed evaluation that the previously applied methods could not find due to their one-sidedness, namely, their attention to technical controls.

Dataset(s) Used

- What dataset(s) were used for experimentation and analysis?
 - They did not use the standard numerical dataset experiment of the kind that you would find in machine learning classes. They rather collected expert voices after conducting interviews with cybersecurity experts in seven sectors of Australian applications(Delphi Method) such as CISOs and top security managers of large organizations. In the process of the interviews those answers became their qualitative data that was analyzed to extract 43 success key variables in eight dimensions
- Are these datasets publicly available, and do they represent the problem space adequately?
 - No, the datasets are not publicly available, as they were created through interviews with cybersecurity experts

Empirical Result

- What experiments were conducted to validate the technique and key metrics used to evaluate performance?
 - In the case of the baseline paper (Yeoh et al., 2023), the empirical findings were the interviews with the experts in the sphere of cybersecurity and the test of the Zero Trust maturity assessment framework. Henrys measured 43 critical success factors (CSFs) based on 8 dimensions on a Likert scale and this resulted in visual charts representing the strengths and weaknesses of the organizations and their readiness to implement Zero Trust in the charts.

Overall Results and Findings

- What are the main findings of the paper?
 - The paper uncovered that to make Zero Trust a successful implementation, it is important to consider eight major dimensions: identity, endpoints, applications, infrastructure, data, networks, visibility and analytics, as well as, automation and orchestration.
- How do the results support or refute the initial hypothesis or research question?
 - The findings reinforce the study questions because they indicate that such critical success factors (CSFs) are able to be organized into a functional maturity evaluation system to allow organizations to recognize their strengths, weaknesses, and areas of emphasis.
- Did the authors discuss any limitations or future work?
 - The shortcomings by the authors included the study had a lock-up qualitative study, and concentrated on Australian experts results and indicated that future research could

broaden the framework with quantitative validation and be more varied and global in an expert panel.

Insights and Critical Analysis

- What are your insights or reflections on the paper?
 - I deduced that the paper provides a practical framework of measuring the maturity of Zero Trust that is actually very useful to organizations in determining their strengths and weaknesses.
- Do you find the methodology and results convincing? Why or why not?
 - Definitely, the methodology is perfect, as the Delphi method is combined with Critical Success Factors (CSFs) to provide a systematic process to gather expert knowledge and develop a maturity framework. However, generalization is not entirely there as the experts were limited to particular regions and industries, which may not be representative globally.
- How could this work be improved or extended in future research?
 - To conduct future research, I believe that it would be excellent to include more different industries/regions/systematic literature support and add some quantitative validation in it as well.
- How does this paper contribute to your own research or the field in general?
 - The paper under discussion is an excellent introduction to my study- it gives me a solid group of CSFs and a maturity model that I can then develop further with an expanded evidence-grounded perspective.

Relevance to Your Research

- How is this paper relevant to your current research focus or thesis?
 - This paper helps in my research because it provides a clear maturity model for Zero Trust, which is directly linked to my research aim of measuring organizational readiness. It provides me with a structured model and set of factors, using that I can build, refine, and augment with further quantitative analysis to produce an organizational model that is more accurate and evidence-based.
- Can any of the techniques or findings be applied or adapted to your research?
 - Yes, the Critical Success Factors and the maturity framework from this paper can be used in my research. Because, instead of only relying on expert opinions which baseline paper does, I plan to enhance the model by using a weighted matrix and quantitative scoring, which will provide a more precise readiness percentage and make the model more practical for organizations.

Baseline Research Paper: Zero trust cybersecurity: Critical success factors and A maturity assessment framework

Link of baseline paper: <https://www.sciencedirect.com/science/article/pii/S016740482300322X>

Our Group Research Topic: “Developing a Zero Trust Readiness Index (ZTRI) to Measure Enterprise-wide Zero Trust Adoption”