Module Code & Module Title

Level 5 – CC5052NI

50% Coursework's

On Zero Trust Architecture

Risk, Crisis, and Security Management

3rd Semester

2024 Autumn

Student Name: Aayush Raj KafleLondon Met ID: 23047570

College ID: NP01NT04A230231

Assignment Due Date: Wednesday, January 8, 2025

Assignment Submission Date: Friday, January 10, 2025

Submitted To: Aakash Ojha

Word Count: 2174

I confirm that I understand my coursework needs to be submitted online via MST Classroom under the relevant module page before the deadline in order for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a mark of zero will be awarded.

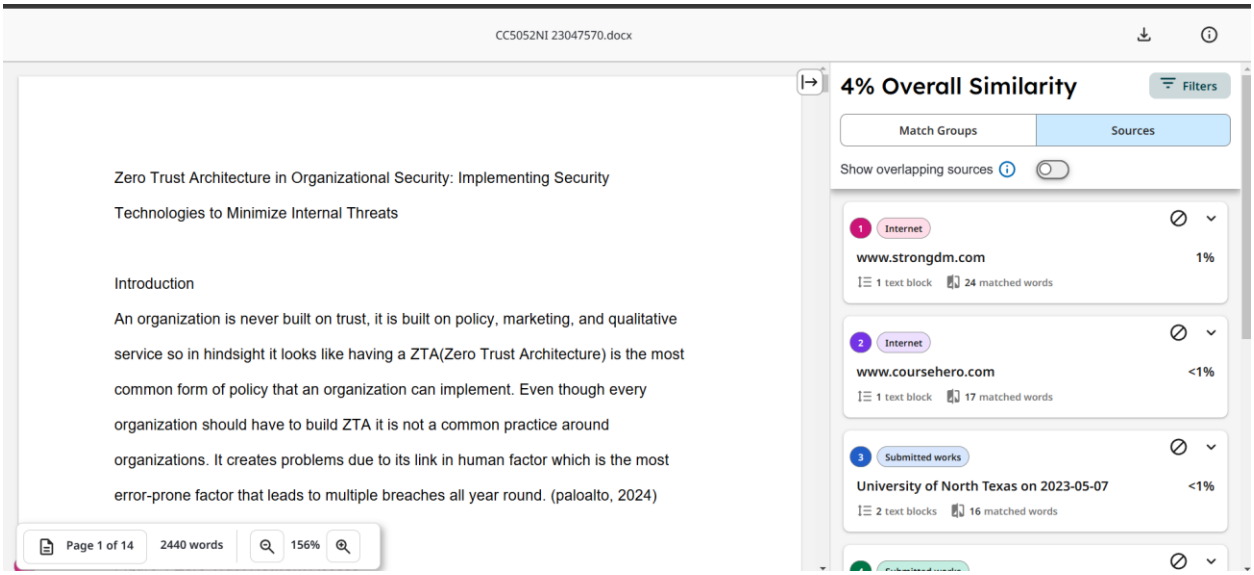

Figure 1 Turnitin Similarity Report After the Filter

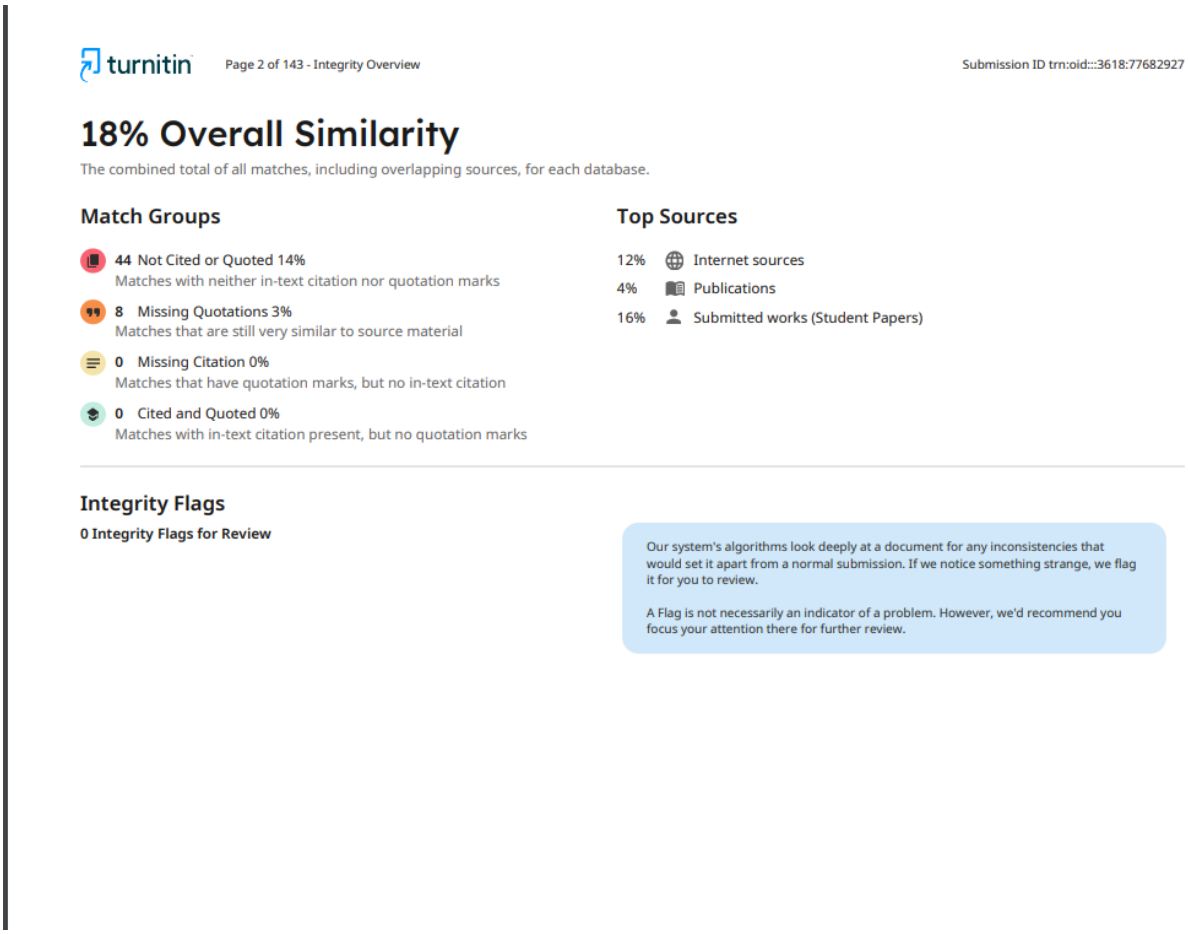

Figure 2 Turnitin Similarity Report Before the Filter

Acknowledgment

I want to extend my heartfelt thanks to Mr. Aakash Ojha for his consistent support and priceless guidance, right from the inception to the completion of this report on Zero Trust Architecture. His extensive experience, thoughtful feedback, and unwavering motivation have formed the backbone of the direction and depth of this work. I am truly grateful to him for his invaluable mentorship. Additionally, I would like to express my gratitude to Apil Chand for his assistance throughout this process. Although his role was more secondary, his timely contributions provided crucial support at key moments, thereby adding significant value to the successful completion of this report.

Abstract

Zero Trust Architecture (ZTA) is a robust cybersecurity framework addressing modern threats by eliminating implicit trust within an organization. Rooted in the principle of "Never Trust, Always Verify," ZTA enforces strict identity verification, least-privilege access policies, and continuous monitoring to mitigate risks associated with insider threats and unauthorized access. This model ensures employees and external users only access resources necessary for their roles, thereby reducing the attack surface and minimizing potential damage from breaches. ZTA aligns with regulatory guidelines, making its adoption not only a security imperative but also a means to avoid hefty penalties.

Despite its proven efficacy, ZTA adoption remains inconsistent across organizations due to human factors, resistance to change, and implementation complexities. High-profile incidents, such as Edward Snowden's 2013 breach of the NSA, highlight the critical need for ZTA. Snowden exploited weak privilege controls and hierarchical gaps to access and leak over 20,000 classified documents. This breach resulted in reputational damage, strained international relations, and significant economic losses, particularly in the U.S. cloud computing industry. If ZTA had been implemented, Snowden would not have been able to bypass strict access controls, reducing the risk of such an incident.

ZTA provides a proactive approach to addressing cybersecurity challenges, from ransomware to insider threats. Its core components—least-privilege access, continuous monitoring, policy enforcement, and regular audits—strengthen organizational security and build stakeholder trust. Additionally, ZTA enhances operational transparency and compliance, creating a secure environment for businesses and governmental entities alike.

In conclusion, the Snowden case underscores the importance of implementing ZTA to address insider threats and strengthen internal security protocols. By prioritizing least-privilege access and rigorous verification, ZTA helps organizations mitigate risks, protect sensitive data, and maintain their reputation in an increasingly vulnerable digital landscape. It is a necessary step toward building resilient and secure IT infrastructures.

Table of Contents

Table of Figures

Zero Trust Architecture in Organizational Security: Implementing Security Technologies to Minimize Internal Threats

1) Introduction

An organization is never built on trust, it is built on policy, marketing, and qualitative service so in hindsight it looks like having a ZTA(Zero Trust Architecture) is the most common form of policy that an organization can implement. Even though every organization should have to build ZTA it is not a common practice around organizations. It creates problems due to its link in human factor which is the most error-prone factor that leads to multiple breaches all year round. (paloalto, 2024)

Figure 3 Zero Trust Network Access

Zero Trust Network Access (ZTNA), sometimes referred to as a "software-defined perimeter," is the most common implementation of the Zero Trust model. Based on micro-segmentation and network isolation, ZTNA replaces the need for a VPN and grants access to the network after verification and authentication. (strongdm, 2024)

In the past many organizations have been exploited due to neglecting in Zero Trust Architecture and had to pay huge settlements due to the clear violation of multiple regulations violation The ZTA piqued my interest when I had to conduct my research about Edward Snowden former NSA intelligence contractor and whistle-blower and how he used his insider knowledge, internal inbuilt relations to leak multipole classified documents revealing the existence of global surveillance programs and multiples countries among which many were global superpower (NBC NEWS, 2014).

1.1) Aims

- this report aims to make sure that at the end of this report and individual making this report is confidently able to determine the factors of ZTA

1.2) Objective

- Analyse the Need and Necessity for Zero Trust Architecture in an Organization
- Assess ZTA's Role in Organizational Security and Reputation
- Identify the Challenges and Opportunities of ZTA Adoption
- Examine the Role of ZTA in Protecting Critical Government Infrastructure

1.3) Rationale

Zero Trust Architecture is a cybersecurity model that is essentially based on the policy "Never Trust, Always Verify." This means ensuring strict access and continuous monitoring to help organizations protect sensitive data against insiders and external threats. Indeed, the Edward Snowden incident in 2013 depicted the catastrophic risks of poor internal security when there was unauthorized exfiltration of sensitive data due to a lack of proper access restrictions, proper monitoring, and escalation procedures. ZTA counters these vulnerabilities through least privilege access, access escalation processes, policy enforcement, regular audits, and adaptive authentication. Had ZTA been in place, Snowden's unauthorized actions would have been detected and prevented. This underlines the strategic imperative for governments and organizations to make ZTA adoption a priority in order to protect operational integrity and retain public confidence in a digitizing world.

2) Literature Review

2.1) Background and History

Stephen Paul Marsh first used trust as measurable and dynamic; his 1994 thesis laid foundational principles to ZTA even though he did not target cybersecurity. The model followed by The Jericho Forum in 2003, and John Kindervag furthered it in 2009 as expressed by Atwell, 2024. In 2010, Google's "BeyondCorp" initiative formally implemented Zero Trust Architecture, securing resource access based on identity rather than traditional perimeter-based security, eliminating reliance on VPNs (IBM, 2024). By 2014, the *Zero Trust Model of Information Security* emphasized "Never trust, always verify," ensuring strict verification for all individuals, internal or external (IBM, 2024). This architecture limits access and privileges, preventing insider threats, privilege escalations, and unauthorized data access.

2.2) Steps to create ZTA

Zero Trust Architecture (ZTA) is an essential framework for addressing modern cybersecurity challenges such as ransomware and other insider threats that underscore its implementation's importance. The principle of "Never trust, always verify." ZTA significantly reduces the attack surface and minimizes the impact of breaches. In addition, the goals of Zero Trust Architecture also align with various guidelines set by different regulatory bodies in the field of cybersecurity; thus, implementing ZTA rather than handling the hefty fines coming from those regulatory bodies would be much easier.

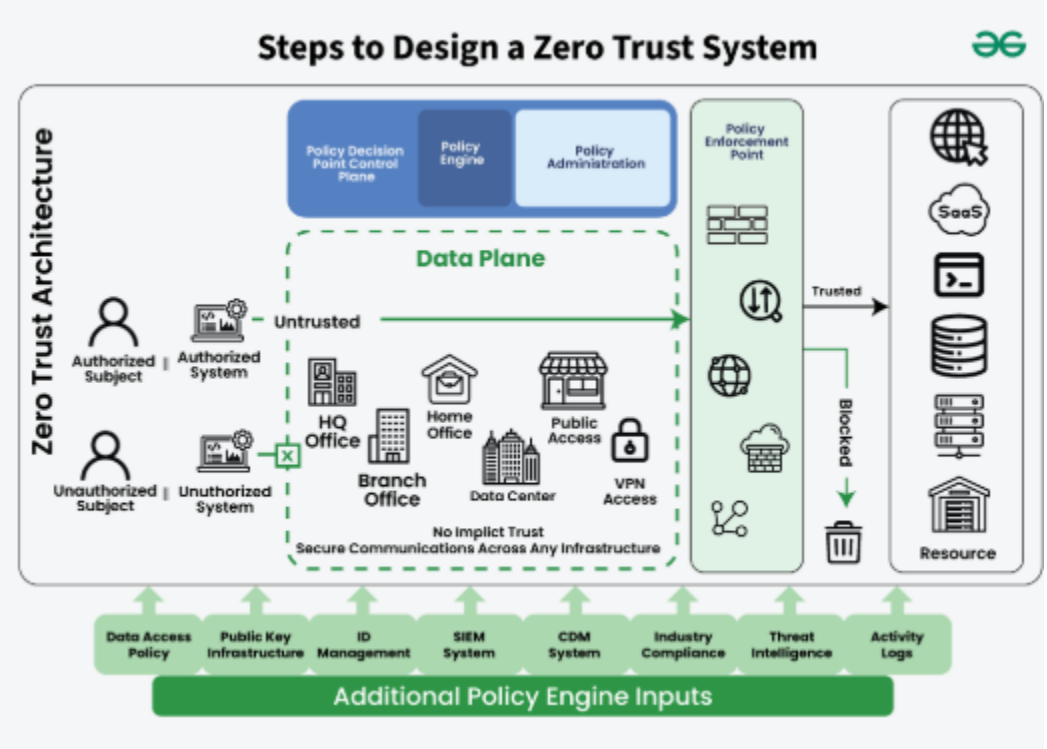

Figure 4 Design of Zero Trust Architecture System

Designing ZTA gives the cybersecurity framework where no user, device, or application can be trusted implicitly inside and outside of a network perimeter. These covers defining the scope and goals through determining the critical assets to be protected, like sensitive data, applications, or systems. First, organizations should analyse their current environment to understand the gaps and risks, and identify concrete objectives, such as protection of remote work or minimization of insider threats. The very basis of Zero Trust Architecture is built on a set of key principles: "Never Trust, Always Verify"; utilization of least privilege access; and the enforcement of micro-segmentation to limit lateral movement inside the network. This, in turn, enhances security posture through continuous monitoring and validation of all activities.

Locking down access points and mapping the flows between users, devices, and resources will help organizations strengthen their security. Strong IAM solutions, including MFA and RBAC, ensure the application of least privilege principles. Micro-segmentation isolates the network into smaller zones, reducing the attack surface, while software-defined perimeters provide encrypted connectivity for authorized entities. Encryption both at rest and in transit, such as protocols like TLS and AES, enhances data security. Data classification, coupled with access control, protects sensitive information. Continuous monitoring and analytics allow for the detection of anomalies and threats in real time, enabled by AI and Behavioral analysis tools. Threats can be mitigated using Security Orchestration, Automation, and Response systems. Training employees on Zero Trust principles, together with periodic penetration testing and policy reviews, strengthens the architecture against any emerging threats and ensures security and resilience across all dimensions.

The basic framework for any organization following ZTA is to assume all external and even newly acquired devices are to be treated as a security concern and be processed as such and follow a proper verification process before granting access to the organizational resources. The other factor of Zero Trust Architecture is access is only granted on a need-to-know basis and least privilege access to each employee to protect the integrity of data. Since 2014 ZTA has gained rapid momentum in many organizational core policies to better protect their digital assets from cyber threats.

2.3) Framework of ZTA

To ensure strict access controls and accountability within an organization, the Zero Trust Architecture (ZTA) framework enforces the principle of "Never Trust, Always Verify" by applying least privilege access policies across all levels, including upper management. No individual, regardless of their role or authority, is granted unrestricted or unlimited access to organizational data and systems. The major Key components in verification that the ZTA remain standing within the organization and continues to do its job are as follows:

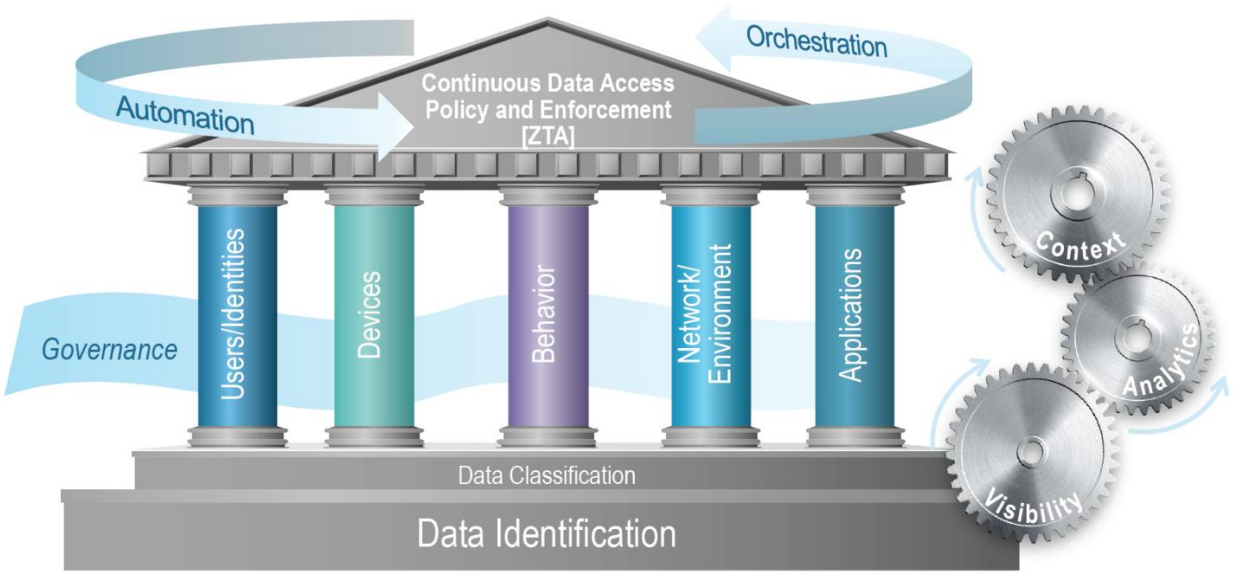

Figure 5 Pillars of ZTA (SHOREPIONT, 2024)

- Least privilege Access

  Limiting the right to access to a minimum while still ensuring it is efficient while maintaining the efficacy of the job to be completed in an orderly time and manner without any problem to arise in the future.

- Access Escalation

  Upper management requires steps to follow before allowing to gain access:

  - Justification and duration on a paper trail.
  - It head/security team approval before gaining higher access than that of their regular pay grade.

- Monitoring and Transparency

  After the approval of the IT head some requirements needed to be completed :

  - Access logged, monitored and reviewed according to the organization's size
  - Must be visible to the compliance officer to prevent any unauthorized access

- Policy Enforcement

  Policy is an invisible rebar that holds the organization's structural integrity. Maintaining proper guidelines and compliance and policy plays an important role in helping prevent any havoc and minimize the chance of ignorance

- Regular Audit

  Outsourcing an external audit team helps maintain compliance stop any violation from occurring and prevent any major scandal and disciplinary action

- Continuous Improvement

  Adaptive authentication, contextual validation, and updates address emerging threats.

3) Methodology and Analysis

The biggest risk for any organization, no matter how strong the security from outside, lies with insider threats. In the absence of internal controls, clear policies, and hierarchical enforcement, individuals with legitimate access can exploit vulnerabilities, leading to catastrophic breaches, as seen in several high-profile cases. Organizations can mitigate such risks by focusing on internal security frameworks and adopting strategies like zero-trust architecture. The case presented below is a perfect illustration of what happens when these measures are ignored and the relevance of structured prevention frameworks.

3.1) Case Study

In June of 2013, Edward Snowden stole the crown jewels of the National Security Agency, and to do that he didn't use any high tech sophisticated or complex vulnerability nor did he develop a new virus to corrupt the NAS system while being undetected all new need was some time to form bonds with right people and few thumb drive to copy the data (Richard, 2013). Without proper verification, process-maintained NAS unnecessary information was shared to the wrong people which led to 20,000 covert documents being gushed out into the world. (The Gaurdian , 2013)

Figure 6 The infamous Edward Snowden

Even though NAS is revered as having one of the best cyber security measures, somehow, that belief was misplaced, as only the technical aspect of organizational security was prioritized. Snowden was able to use his influence over multiple people who held power and authority over secretive documents and governmental prototypes like Prism. (Richard, 2013). Due to his action the NAS and the US government faced an immediate huge backlash which hampered their reputation and public relations. The leaks also hampered relations between Brazil and Ecuador with as one cancelling a state visit and another one renouncing US trade benefits. Some IT companies we subjected to massive financial backlash and other secure email providers had to close due to NSA and other government pressures to reveal their secret keys. the current estimation is that the US will lose between 25 billion to 35 billion in cloud computing-based revenue due to Snowden's leaks. (Heerden, 2015)

3.2) Reflection

The Snowden breach in the NSA underlined critical gaps in internal security, as it came to light that while external defences were robust, internal policies failed to check an insider from leaking classified information. This underlined the need for strong insider threat management and strict access control with continuous authentication. Lax internal policies pose serious risks even to government entities and smaller organizations. Such threats can be mitigated only by adopting Zero Trust Architecture. The principle of "Never Trust, Always Verify," micro-segmentation and continuous monitoring done by ZTA secures the sensitive data from both internal and external threats. Governments dealing with critical information have to keep ZTA adoption at the forefront to prevent insider threats and safeguard national security.

3.3) Prevention using the given framework

The leak made by Snowden opened the eyes of many governmental agencies around the world to make them maintain a strict hierarchy in the organization that chain should not be broken, and a strict formation of data sharing should be maintained to prevent such disasters in the coming future,

Some measures that would have been effective in preventing such mishaps are :

1. Least Privilege Access

   If Least Privilege Access mode was utilized, then Snowden wouldn't have had access to programs classified beyond his role as it would have restricted data other than those to perform his job.

2. Access Escalation

   This could have blocked Snowden’s access to sensitive files as it would have required documented justification and multi-tier approval for elevated access

3. Policy Enforcement

   Enforcing clear security protocol with clear consequences for violation would have deterred any attempts to violation

4. Regular Audits

   External sources would have been handy to know if someone like Snowden was gaining access to information they were not supposed to gain accessed to.

5. Continuous Improvement

   Other advanced measures are adaptive authentication, behavioural analysis, and data classification that further complicate attempts to bypass controls and reach sensitive data.

6. Monitoring and Transparency

   Real-time access to monitoring would have shown when Snowden transferred a large file across device which could have been flagged as suspicious and have been prevented if continuous monitoring had been done.

Conclusion

Zero Trust Architecture acts as a strong base for any organization in order to reduce insider threats and have good security mechanisms in place. Emphasizing "Never Trust, Always Verify" and least-privilege access, ZTA minimizes vulnerabilities across the systems, ensuring that any individual of the position one holds-can have access to only what is deemed necessary for their roles.

The Snowden case study shows the disastrous outcome of not taking care of such principles. Snowden took advantage of the NSA's internal hierarchy and privilege management weaknesses, which needed to be strictly controlled and continuously monitored. If ZTA had been in place, this unauthorized access and subsequent data leak could have been avoided.

This report concludes that ZTA adoption is not only a preventive measure but also a strategic necessity for sensitive data protection, public trust, and regulatory requirements. It calls for the highest priority to be given by governments and organizations in adopting ZTA to protect against insider and external threats for operational integrity in an increasingly interconnected and digital landscape

Appendix

A Future-Ready Security Model for Organizations

Zero Trust Architecture has reach across multiple industries as any organizations following ZTA's policies and rules has much less to lose and can gain trust of multiple potential investors as an outstanding security policy and wok ethics is a common selling factor to gains investment. It also offers solutions to many hidden problems in the organization that will pop its head in the future.

With data breaches continuing to get more and more expensive, Zero Trust Architecture is one proactive security model that's ready for the future. Understanding this topic would enable me to understand and design robust systems that can ward off emerging cyber threats with a view to assuring a safer digital environment.

References

Atwell, E., 2024. *1password.com.* [Online]
Available at: https://blog.1password.com/history-of-zero-trust/#:~:text=The%20term%20%E2%80%9CZero%20Trust%20Model,to%2Dday%20responsibilities).%E2%80%9D
[Accessed 29 11 2024].

Heerden, S. v. S. a. R. V., 2015. *The Consequences of Edward Snowden NSA Related Information Disclosures.* [Online]
Available at: https://www.researchgate.net/publication/275019554_The_Consequences_of_Edward_Snowden_NSA_Related_Information_Disclosures
[Accessed 30 11 2024].

IBM, 2024. *The Evolution of Zero Trust and the Frameworks that Guide It.* [Online]
Available at: https://www.ibm.com/think/insights/the-evolution-of-zero-trust-and-the-frameworks-that-guide-it#:~:text=Zero%20trust%20began%20in%20the,traditional%20perimeter%2Dbased%20security%20model.
[Accessed 29 11 2024].

Marsh, S. P., 1994. *Formalising Trust as a Computing Concept,* Stirling: University of Stirling.

NBC NEWS, 2014. *NBC news.* [Online]
Available at: https://www.britannica.com/biography/Edward-Snowden
[Accessed 28 11 2024].

paloalto, 2024. *paloaltonetworks.com.* [Online]
Available at: https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture
[Accessed 28 11 2024].

R. E. M. C., 2013. *How Snowden did it.* [Online]
Available at: https://www.nbcnews.com/news/world/how-snowden-did-it-flna8c11003160
[Accessed 29 11 2024].

SHOREPIONT, 2024. *ShorePoint's Innovative ZTA Framework and Agile Implementation Methodology.* [Online]
Available at: https://shorepointinc.com/shorepoints-innovative-zta-framework-and-agile-implementation-methodology/
[Accessed 30 12 2024].

strongdm, 2024. *What Is Zero Trust Architecture?.* [Online]
Available at: https://www.strongdm.com/zero-trust
[Accessed 30 12 2024].

The Gaurdian , 2013. *Edward Snowden: the whistleblower behind the NSA surveillance revelations.* [Online]
Available at: https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance
[Accessed 30 12 2024].