

UNIVERSITY OF WALES (TSD)
LONDON CAMPUS.

Name - RAPHAEL JERRY APPONSAH APPIAH

Student id. - 2337090

Module name =. DATA SECURITY AND COMPLIANCE

Code =. (ACCA 5034)

Course name = BSc. APPLIED COMPUTING

Lecturer Name =. Dr. AYMAN AI HAJJAR

Submission Date = 11 / 08/ 2026

Table of Contents

TASK 1-RESEARCH IN DATA SECURITY AND COMPLIANCE

A Critical Analysis of Zero Trust Architecture.

I.	Abstract	3
II.	Introduction	4
III.	Principles of Zero Trust Architecture	4
IV.	Anticipating cyber-Threats	5
V.	Protecting Information Assets	5
VI.	Detection of Security Incidents	6
VII.	Automated Response to Threats	7
VIII.	Implementation Challenges	8
IX.	Comparison with Traditional Security Models	9
X.	Critical Evaluation	10
	Conclusion	10

TASK 2 – Designing a Structured and Forward-Looking Cybersecurity

Programme For Equifax.

I.	Introduction	10
II.	Organisational Structure and Accountability	10.
III.	Vulnerability and Patch Management Policies	11
IV.	Secure Software Development and asset Management	12
V.	Governance and Strategic Alignment	13
VI.	Risk Management and High – Level Risk Assessment	14
VII.	Regulatory Compliance and Breach Notification	16
VIII.	Incident Response, Disaster Recovery	17
IX.	Technical Safeguards	18
X.	Conclusion	19
	References	20

TASK

Research in Data Security and Compliance

Title. A Critical Analysis of Zero Trust Architecture ; Principles, Implementation Challenges, and Effectiveness Compared to Traditional Security Models

Abstract ;

Zero Trust Architecture (ZTA) has become an innovative framework of cybersecurity for overcoming the shortcomings of traditional security approaches for cloud computing, hyper environment and remote work. This research aims to perform a critical evaluation of the key aspects of ZTA. Including continuous verification, least -privilege access, and continuous monitoring, along with assessing its efficiency in terms of being able to foresee, defend from, and react on cybersecurity attacks. The current paper will also explore the issues related to implementing ZTA such as compatibility with legacy systems, deployment difficulties, and expenses while comparing the features of ZTA with the characteristics of traditional security approach. In conclusion, Zero Trust Architecture appears to be achieved by organizations that a substantial amount of resources spent.

INTRODUCTION

Modern enterprises exist in a constantly changing business environment characterized by Cloud computing remote working conditions, and the ubiquitous use mobile device difficult . These changes have significantly enlarged the network perimeter, making it increasingly

companies to effectively secure vital organizational assets using conventional security systems . Perimeter security which operates on a notion of intrinsic trust among all

network members , has become an insufficient method to counteract modern cyber all attackers , such as insider threats, identity thief's, and advanced persistent threats.[1] [2]. To overcome this situation, organizations need more sophisticated solutions to address new realities of digitalization .

Zero trust Architecture (ZTA)has been designed to solve these issues. Based on the principles of “never trust always verify “ this approach eliminates implicit trust , by continuously verifying the identities of user, devices, and applications before providing them with access to company assets.[1] ,[3]. Identity – centric security , least – privilege access control, and continuous monitoring help minimize risks and limit malicious activities inside a network. The present paper provides an analysis of their strengths and weakness of the Zero Trust Architecture..

❖ Principles Of Zero Trust Architecture ;

Zero Trust Architecture is based on a range of key principles that redefine access management in today companies . The first principle differentiates zero trust approach from the traditional network security concept in that there is no longer any presumption about implicit trust within a certain network boundary. Instead , Zero Trust assumes that no user and no device should be trusted automatically , regardless of location – an issue of increasing relevance amid widespread use of cloud service , remote working , and mobile devices. Another principle of zero trust architecture is continuous verification . Under the zero trust paradigm , each access request needs to be authenticated and authorised before providing access . Here , the validation concerns such aspects as the user identity and the device used , as well as contextual information about location and behaviour. Continuous

verification occurs during each session since authentication continuous until the end of the session.

necessary to do his job properly . With this implemented , the possible harm caused by insider and compromised accounts will be drastically reduced.

The practise of micro- segmentation also provide enhanced security . It involves splitting the network into multiple isolated sections. By doing so , an attacker who gain access to one computer would have more difficulties moving laterally across the system to gain access to another computer.

Finally , device and identity security are among the key element in building zero trust architecture . Multifactor authentication , endpoint verification , and identity verification are necessary to guarantee that only trust users and devices get access to the resources . The national institute of standard and technology states that zero trust involves ongoing monitoring and verification of trust levels for all entities engaging with system .[1] ..

The principles combine to form a strong and flexible security structure well – suited for contemporary digital landscapes.

❖ Anticipation Of Cyber Threats ;

By employing the zero trust models of operations based on the presumption of breaches , originations become more capable of anticipating the cyber threats. While relying on reactive security controls ineffective against modern attacks , ZTA allows adopting a proactive approach towards security , constantly assessing the risks and discovering the vulnerabilities before their exploitation by cyber criminals.

One of the key method helping to active the goal is the incorporation of threat intelligence into security controls of an organization . In doing so, an enterprise receives a comprehensive view of both existing and emerging g cybersecurity risks associated with attacks, vulnerabilities and actors by analysing threats intelligence from various sources . In addition , risk- based authentication serves as a means to anticipate cyber attacks. Through analysis of different contexture variables, such as using identity , type of device used for accessing sensitive resources , time of accessing , and behaviour , security systems assign dynamic risk sensitive data. Another technique used by organizations to anticipate threats is behavioural analytics . The use of artificial intelligence

and machine learning techniques helps detecting abnormal behaviour that. might indicate some malicious activities.[4]. It could involve unusual access attempts or data transfer something else.

❖ Protection Of Information Resources ;

The security in ZTA is based on tight access control policies and a layered defence approach that aims to limit the potential threats exposure to the resources . While most security solutions place their focus on perimeter defences , ZTA seek to secure each resources by validating each attempt to access the resources. Therefore, the sensitive data is protected from any unauthorized access and usage regardless of the user physical locations . One of the primary mechanisms used to ensure the security of resources under ZTA is identify and access management (IAM) . IAM is responsible for managing user authentication and authorization process, including implementing RBAC or ABAC policies , limiting the amount of exposure to potential threats and risks. In addition to IAM , organizations must implement MFA policies, which include a combination of different factors used for identifying the user. In particular , MFA involves password bases, biometric, or code –based authentication techniques. Such a policy will allow the organization to strengthen its security posture and mitigate ant potential threats, including those arising from login credential thefts.

Data Lose Prevention (DLP) solutions are crucial when it comes to protecting sensitive information resource. These policies aim to ensure proper monitoring , detection , and blocking of any unauthorized attempts to transfer , store, or access sensitive data. Such policies enable organizations to limit potential risks associated with data leakage and misuse.

Finally , organization can use endpoint security validation policies to control the access of endpoint to sensitive data. These policies help ensure that each device meeting all security requirements before connecting the access of potentially vulnerable devices to critical systems and resources. Overall , these four components from the basin of a strong security control framework that allows organizations to minimize the likelihood of unauthorised access or data breaches.[3].

❖ Security Incidents Detection;

Security incidents detection serves as one of the fundamental components of ZTA , allowing organizations to detect and address security incidents in real –time . Unlike conventical security strategies based on scheduled monitoring or perimeter- based alerting solution , ZTA assumes constant monitoring of all users , devices and network communications, leading to the earlier detection of threats and reducing their possible impact.

One of the essential means of achieving this goal lies in this usage of security information and event management (SIEM) systems. SIEM products consolidate information about the

security status from various sources, including servers , applications, and network equipment . The analysis of logs and events provided by them results in the centralized visualization of alert in case of detected abnormalities or threats.

In turn , another technology , namely , user and entity behaviour analytics (UEBA)focuses specifically on analysing behavioural patterns. Using the baseline established beforehand , the systems identify and changes indicating malicious intent, like atypical times of logins , unusual data access operations, or unauthorized privilege attempts. It allows them to identify not only external attacks but also the actions of insiders or compromised accounts that bypassed other security controls.

Overall , all of these technologies ensure that a company gains insight into its security status and detection anomalies , thus enhancing the efficiency of zero trust compared to traditional security practice .[5]

❖ Automatic Reaction To Threats;

Automated responses represent another benefit of ZTA in relation to modern cybersecurity problems. With the growing speed and complexity of attacks, manual reaction measures become increase insufficient to prevent advance effects. The problem can be solved by including automated reaction mechanising in ZTA . Such approaches ensure real-time detection , analysis, and response time and preventing threats from causing damage. For example, one of the most common ways of responding to attacks is automatic session termination . Once an account shows sign of abnormal behaviour , the connection can be terminated instantly . If a user accesses sensitive information and an unusual pace or from

Access restrictions also play an important role in responding to attacks . The process involves dynamic modification of a users access rights pending on their risk level . If a person demonstrate suspicious behaviour, then they receive restricted access to certain

In general, automation plays a significant role in making incident response faster and more consistent through ZTA implementation.[6].

❖ Implementation Challenges;

While being beneficial , however , the introduction of zero trust architecture (ZTA) posers quite a number of problems for many organizations . They move from legacy approaches to zero trust involves considerable effort, experiences , and difficulties associated with both technical issues and organizational specification .

One of the major barriers to implementing the model is compatibility issues. As many existing information systems rely on out of date technologies incompatible with continuous verification and fine-grained control principles, their adaptation for usage in a zero trust setting might turn out to be rather difficult and expensive, sometimes unfeasible at all. In these cases, organizations will have to invest into upgrading or even replacing the system in question. The second problem is represented by high costs related to introducing and maintaining a new security architecture. Apart from purchasing various tools needed for building and running ZTA, such as identity verification software and automation platforms, companies will incur considerable additional expenses connected with personal training and other aspects of implementation and upkeep. For small enterprises, such as costs may be hardly manageable ..

One more difficulty is related to lack of specialists. To implement and manage zero trust systems efficiently, companies will require experts capable of designing and deploying secure solutions. Based on the latest advances in cybersecurity, identification, and data protection. Yet there is currently an insufficient amount of qualified personnel available on the market due to growing interest in information technology in recent years.

Lastly, another potential issue may be opposition arising among employees and management. Such resistance might be caused by discomfort associated with increased complexity of working or even just unfamiliarity with zero trust principles. All mentioned factors shall be taken into account in order to ensure successful implementation of ZTA [2].

❖ Comparing ZTA To Traditional Security

Models;

that a system can be considered safe and secure since its components are operating in an environment defined by clear boundaries within a single organization. In zero trust architecture case, however the environment is more distributed.

Proactivity that comes as part of zero trust can be cited as the most important strength of this concept. Unlike traditional approaches to security that rely on threat identification and mitigation after an event, zero trust architecture continually analyses the risks and applies security policies in a timely manner. The result is shrinking of the attack surface and limitation of opportunities for lateral movement of the adversary in the network.

Additionally, focusing on identification rather than locations, zero trust architecture fits into today's reality, where people use many devices and locations to access systems. To summarize, zero trust provides more flexible and resilient security than traditional approaches.

❖ Critical Evaluation ;

Zero Trust Architecture is considered as one of the most innovative and effective cybersecurity frameworks applicable to modern organization , overcoming the limitation of traditional security models based on a concept of a perimeter. The “ never trust , always verify” approach makes it possible to enhance significantly the security posture of an enterprise. Still , although zero trust offers a range of benefits , there are some challenges connected with its use .

One of the key strengths of Zero trust architecture is its capability to address problems caused by insider threats. Conventional security models usually operate under the assumption that all network users are trustworthy , which can result in attacks from the insider of the system. In construct, continuous verification of the identification of users and enforcement of the principle of least privilege help minimised the risk of compromising sensitive information and limit lateral movement inside the network.

Enhanced visibility and ability to monitoring the network constitute another benefit offered by and responds to them in time. It should be noted that ZTA is well –suited for hybrid or remote workforces. Nowadays , employees of an organization can access its resources from various locations using various location , using various devices . Hence, zero trust is very relevant as it allows establishing a secure connection based on identity and device verification rather than network location.

However, there are also several weak sides associated with zero trust. To begin with the development of this hold may be complicated , as it usually involves not only the reengineering of the numerous security technologies and the formulation of access policies.

Also , implementing ZTA often requires significant investments in such technologies as IAM, monitoring systems, and automation tools.

Finally , Zero Trust requires constant management to ensure efficient operation . Policies need to be regularly reviewed to update them and check the security status of the system to prevent mis configurations. Taking this into account, a phased implementation of Zero Trust may be recommended.

Conclusion

1. The concept of zero trust architecture, is a major shift in today cybersecurity strategies moving from the traditional approach of protecting internal network resources with perimeter defences to more proactive and identity – focused model.

The reality of the modern technological environment, which features ubiquitous use of cloud computing, remote work, and networking , goes not allows any assumptions about inherent security insider corporate systems anymore. Thus , zero trust architecture addresses these challenges through constant verification, enforcement of least – privilege policy , and monitoring of all users, devices , and applications.

As show in this paper, the adaption of zero trust allows organization to be better prepared for modern cybersecurity attacks in terms of preventing, protection, detection , and response actions.

Task 2

Designing a Structure and Forward – Looking Cybersecurity Programme for Equifax

Introduction

The 2017 Equifax data breach can be used as a classical example demonstrating how poor cybersecurity governance can turn an existing preventable vulnerability into a critical organisational crisis. Equifax is one of the largest us-based consumer credit reporting agencies holding very sensitive information about millions of people. Hackers too advantage of the vulnerability in the Apache struts farmwork that was being used in Equifax online. Automated consumer interview system and gained unauthorised access to sensitive customer information, including personal data such as name, address, date of birth, social security numbers, and in some cases, payment card information. According to the United States Government Accountability Office, hackers manage to obtain information about at

lease 145.5 million customers with subsequent regulatory disclosures stating that there were approximately 147 million affected customers [7], [8]

These intruders stayed on Equifax's network for 76 days before discovery. The investigations revealed the lack of proper asset identifications, vulnerability management, certificate management, network segmentation, monitoring, and data governance [7]. Therefore, it was not a case of a single administrator forgetting to deploy a certain patch. An effective forward- looking program should include executive governance, policies and metrics ongoing risk assessment s, secure design of systems, and incident response planning.

2.2 Organizational Structure And Accountability

It is essential that cybersecurity is viewed as a risk at the enterprise level rather than just an IT risk. A major security event could have ramifications for regulatory compliance, reputation , consumers trust, continuity of operations, and profitability. Therefore, accountability needs to expand beyond the operational staff to senior management and the board

2.2.1 Proposed Government Structure

ROLE	PRIMARY RESPOSIBILITY	REPORTING LINE
Board Risk and cybersecurity committee	Endorses cybersecurity plan, funding, risk tolerance, and critical risk choices.	Board of Directors
Chief Executive officer	Responsible for the overall executive oversight of organizational security.	Board of Directors
Chief information security officer	Manages security governance, risk, compliancey , and incident response	CEO and Board committee

Chief information officers	Oversees technology operations, infrastructure, and service provision .	CEO
Security Architecture manager	Sets up a secure framework, division ,and technological guidelines	CISO
Vulnerability and Patch manager	Coordinates reviewing, fixing, and confirming remediation	CISO
Internal Audit	Assesses cybersecurity governance and control autonomously	Audit committee.

It is necessary for the chief information security officer (CISO) to report directly to the chief Executive officer (CEO) and be able to access the board risk and cybersecurity committee without any restrictions. It means that the security leadership will have enough power to question inappropriate decisions and escalate risk. If the CISO reports to the chief information officer (CIO)only, security issues can be overshadowed by considerations of services availability, project schedules, or financial goals.

CISO and CIO position should not be merged. CIO is responsible for providing reliable and efficient information systems, but the role of CISO include independent assessment of security of these systems. The merging of these positions can create a conflict of interest. When the same executive evaluates the security of his or her decision regarding the system delivery.

The RACI matrix should be used in terms of accountability. For example, when the existence of critical vulnerability has been announced, the vulnerability manager is responsible for the identification of affected assets. System owner is accountable for the completion of remediation, security operations centre needs to be consulted about position active exploits , and the CISO should be informed about delays. The board needs to be provided with cybersecurity reports once per quarter, whereas security performance should be discussed with executive management once per month. Report includes;

1. amount of unknow or unsupported assets.
2. Critical vulnerabilities and overdue patches.
3. Significant security incidents.

4. Third – party and supply chain risks.
5. Failure or unavailability of security controls.
6. Mean time to be detect and contain incidents
7. Implement of the existing security plans.

Failure of the critical controls needs to be reported immediately and not to wait for the scheduled meetings, it will help avoid the division of responsibility for patching, monitoring, and system ownership from becoming fragmented across departments.

2.3 Policies and Procedures;

Security policies have to be clear, measurable, auditable and enforceable. Instructions like “patch systems promptly will not work. Every policy has to be specific regarding its scope, owner, mandatory requirements, performance measures, exception process, and non-conformance consequences.

2.3.1 Vulnerability Management Policy;

Vulnerability management policy obliges the organization to identify assess, prioritize

And remediate vulnerabilities associated with servers, applications, endpoints, network devices and cloud services. Check of vulnerabilities have to be run weekly on internal systems and daily for critical internet – facing resources. Scans should also be carried out after significant changes in configuration or after disclosure of a critical vulnerability.

There has to be taken into account such factors as follows

- Presence of internet facing assets.
- Indications of actual exploitation of a vulnerability.
- Sensitivity of data handled by the asset.
- Significance of the asset for business processes.
- Presence of compensatory controls,
- Possible regulatory and reputation implications.

Therefore, a critical vulnerability in an internal facing application handling consumers data should get a higher priority than an equivalent vulnerability in a stand- alone testing environment. All vulnerabilities should be registered in one vulnerability register where such data have to be specified ; affected assets, system owner, action required, remediation deadline and proof.

2.3.2 Patch Management Policy;

Equifax case has shown that just giving a command to apply a patch does not always mean remediation of a strut's vulnerability has been distributed internally, but Equifax did not find the vulnerable application [7] , [8]. According to NIST, enterprise patch management has to be considered as preventive maintenance and a necessary function for the organization and not an optional task [14] . The following service- level targets have to be up the policy.

Vulnerability Category.	Maximum remediation period
Activity exploited critical vulnerability	72 hours
Internet – facing asset	
Other critical vulnerability	7 days
High – risk vulnerability	14 days
Medium – risk vulnerability.	30 days
Low – risk Vulnerability.	90 days

However, emergency patching processes need to allow for any change that can be done quickly without holding an ordinary change management session. However, any emergency patch still needs to in testing, approval, documentation, and rollback process. If the patching cannot be done at once, some protective measures need to be taken as well. This might include stopping the exposed service, quarantining the machine, limiting internet access, creating a WAF rule, or increasing monitoring. The patching exception requires needs to indicate the reason for the delay, control measures, risk, owner, and final remediation deadline. Important exceptions need to receive approvals of both CISO and senior business executive. Compliance evaluation needs to be done on the basis of patching rate, amount of overdue vulnerabilities, and average remediation time.

2.3.3 Secure Software Development Lifecycle Policy;

The consideration of security factors needs to be incorporated in the entire software development process as opposed to being considered exclusively before software is deployed. According to NIST secure. Software development framework, it is important to incorporate security into every step of the software development lifecycle to minimize the number of vulnerabilities [15] . In order to deploy secure development practice;

- ❖ Security and privacy requirements determined in the planning process.
- ❖ Threat Madeline of critical applications.

- ❖ Incorporation of secure coding standards approved by the organization.
- ❖ Peer review of the code.
- ❖ Static application security testing.
- ❖ Software composition analysis.
- ❖ Penetration testing prior to major release.
- ❖ Security approval before production deployment.

Software composition analysis is especially relevant to the current situation since modern applications rely on many open- source and third – party components. In order to help Equifax recognize application that use the vulnerable versions of components like Apache struts All developers should receive training on secure coding annually, and development teams need to avoid using real consumer data for testing purposes unless it is justified and there are appropriate measures implemented.

2.3.4 Asset Management Policy;

The organization cannot protect its systems without having them properly identified. As a result, the organization shall keep on up to date inventory consisting of servers, users workstations, application, databases, cloud infrastructures, network devices, software, and internet access, between domains. The inventory record of each asset should contain the following.

- Business Owner
- Technical Owner
- Location cloud or physical)
- Software and OS versions
- Status of Support
- Classification of data and it processes.
- Critically of the asset for business operations
- Whether it is external exposed

Automated discovery solutions should perform periodic comparison of discovered activity on network and in the cloud with the inventory. An unknown asset should create an investigation ticket. This asset records should be periodically updated based on procurement data, network scans, cloud platforms, software repositories, and configuration management systems. According to the CIS critical security control, the inventories of enterprise assts and software are considered to be fundamental controls, as other security functions like patch management, monitory, and incident response rely on proper visibility [16]

2.3.5 Monitoring and Logging Policy;

Security- related logs should be centrally collect in a security information and event management (SIEM) solutions, applications, databases, endpoints, servers, firewalls, cloud platforms, and network monitoring solution. According to empirical analysis of Equifax , the expiration of a digital certificate had an effect of preventing the monitoring solution from analysing the encrypted traffic, after renewal, previously concealed traffic become visible [7]. Thus, the certificate lifecycle management with the help of automated solutions and timely notification about the certificate expiration should be put in place.

2.3.6 Policy for Protecting Policy and Access.

Personal data should be collected and stored only when needed for legal and business purposes. Equifax should priorities its data based on the sensitivity of the information collected and give the top priority of the information collected and give the top priority to such categories of data as social security numbers, financial and identity information.

2.4 Government and Strategic Alignment;

The cybersecurity program needs to be consistent with the NIST cybersecurity Farmwork 2.0. The farmwork permits organization to effectively communicate and manage their cybersecurity risk through six primary functions, Govern, Identity, Protect, Detect, Respond, and Recover [4]. The govern activity ensures that decision- making related to cybersecurity is aligned with the overall business strategy of Equifax and the level of acceptable risks and compliance needs. Using

Using NIST CSE Current and Target Profiles, enable the organization to recognize deficiencies and create prioritized plans for improving them in terms of who will do what , budgeting and deadlines. Furthermore, NIST SP 800-and CIS Controls can provide a complete set of protections whereas quantitative metrics for asset visibility, patching, authentication, detection , containment, and recovery will show the effectiveness of security spending [11], [16].

2.5 Managing and Evaluating Risks;

Assess cybersecurity risks based on the probability of exploitation and the impact on confidentiality, integrity , availability, legal adherence, and organizational standing.

2.5.1. High – Level risk assessment;

Risk	--	Likelihood -	impact	Priority	- Proposed mitigation
Unpatched internet		very high	Critical	1	Rapid patching ,scanning
Incomplete asset inventory	/	High /	Critical	2	Continuous discovery and asset-owner
Weak network segmentation	/	High /	Critical	3	Restricted database access
Compromised privileged account	/	High /	Critical	4	MFA, access management monitoring
Failed monitoring controls	/	High /	High	5.	Tool checks and certificate management
Vulnerable third party software	/	High /	High	6	Component analysis and software inventory
Excessive data retention	/	medium /	Critical	7	Data minimisation and secure deleting
Ineffective incident escalation	/	medium /	Critical	8	Exercises, defined escalation.
Insider misuse	/.	Medium /.	High	9	Least privilege, monitoring and access review
Ransomware	/.	Medium /	Critical	10	Endpoint detection, immutability backups

The rationale behind this assessment is to prioritise threats which can potentially result in exposure of sensitive data or disruption of services. High-priority threats include things like lack of patching for systems exposed to the internet and insufficient asset visibility. Principles of Zero Trust should also be incorporated to minimise the dependency on network as an indicator of trust . Every single access attempt must be authenticated and authorized according to identity and context [12].

2.6. Compliance, Incident Response, and Protection Controls

The section below provides a description of the approach of the company in terms of the management of security incidents, compliance, and technical controls aimed at protecting systems and data

2.6.1 Compliance and Notification of Security Breaches;

This sub-section provides information on the processes of identification, reporting , and communication of the security breaches according to the legal requirement. Equifax must have documented procedures on breach notification in all jurisdictions in which the organization operates.

2.6.2. Incident Response;

This sub – section provides details of the process of detecting containing and recovering from cybersecurity incidents. Incident response must follow the formal lifecycle including preparation, detection, containment, eradication, recovery, and post- incident activities [7].

2.6.3 Disaster Recovery and Business Continuity;

This sub- section provides information about the processes and approaches to the recovery of critical system after disruptions and provision of essential services throughout the recovery period.

Procedures related to backup and recovery of systems should be tested regularly to ensure reliability and security of system recovery.

2.6.4. Technical Safeguards;

This sub-section provides information on the technical security controls applied by the company to protect systems, detect and prevent attacks

CONCLUSION.

This section summarizes the key learnings from the Equifax incident and highlights the importance of having structured governance, risk management, and technical controls. Unlike a technological flaw that was not possible to avoid, the Equifax incident shows flaws in governance, asset management, patch management, and monitoring. The suggested cybersecurity program addresses the mentioned flaws through accountability, policies, prioritization based on risks, and following the framework of the NIST Cybersecurity Framework 2.0. The use of structured governance and continuous monitoring, as well as technical controls, significantly reduces the chances and impacts of such events in the future

REFERENCE

Bibliography

- [1] National Institute of Standards and Technology, "Zero Trust Architecture," National Institute of Standards and Technology, Gaithersburg, MD, 2020.
- [2] S. Rose, O. Borchert, S. Mitchell and S. Connelly, "Zero Trust Architecture Design Principles," *IEEE Security & Privacy*, vol. 18, no. 3, pp. 34-41, 2020.
- [3] E. Gilman and D. Barth, Zero Trust Networks: Building secure Systems in Untrusted Networks, Sebastopol, CA: O'Reilly Media, 2017.
- [4] R. Ward and B. Beyer, "BeyondCorp: A New Approach to Enterprise Security," ; *login.*, vol. 39, no. 6, pp. 6-11, 2014.
- [5] European Union Agency for Cybersecurity(ENISA), "Zero Trust Architecture Overview," European Union Agency for Cybersecurity(ENISA), Athens, 2021.
- [6] J. Kindervag, "Build Security into Your Network Architecture," Forrester Research , Cambridge, MA, 2010.
- [7] U.S Government Accountability Office, "Data Protection :Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach," U.S Government Accountability Office, Washington, DC, 2018.
- [8] U.S . House of Representatives, Committee on Oversight and Government Reform, "The Equifax Data Breach," U.S House of Representatives, Washington ,DC, 2018.
- [9] Federal Trade Commission, "Equifax to pay \$575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach," Federal Trade Commission , Washington , DC, 2019.

- [10] National Institute of Standards and Technology, "The NIST Cybersecurity Framework (CSF)2.0," National Institute of Standards and Technology, Gaithersburg, MA, 2024.
- [11] National Institute of Standards and Technology, "Security and Privacy Controls for Information Systems and Organizations," National Institute of Standards and Technology, Gaithersburg, MA, 2020.
- [12] R. S, B. O, M. S and C. S, "Zero Trust Architecture," National Institute of Standards and Technology(NIST), Gaithersburg, MD, 2020.
- [13] National Institute of Standards and Technology, "Incident Response Recommendations and Considerations for Cybersecurity Management:A CSF 2.0 Community Profile," National Institute of Standards and Technology, Gaithersburg,MD, 2025.
- [14] M. Souppaya and K. Scarfone, "Guide to Enterprise Patch Management Planning :Preventive Maintenance for Technology," National Institute of Standards and Technology (NIST), Gaithersburg, MD, 2022.
- [15] M. Souppaya, K. Scarfone and D. Dodson, "Secure Software Development Framework(SSDF)Version 1.1:Recommendations for Mitigating the Risk of Software. Vulnerabilities," National Institute of Standards and Technology (NIST), Gaithersburg, MD, 2022.
- [16] Center for Internet Security, "CIS Critical Security Controls Version 8," Center for Internet Security, East Greenbush, NY, 2021.