International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7178
***Article Received**: 22 April 2023 **Revised:** 10 June 2023 **Accepted:** 25 June 2023*

A Novel Cyber Resilience Framework – Strategies and Best Practices for Today's Organizations

A. Kanthimathinathan[1], Dr. S. Saravanan[2], Dr. P. Anbalagan[3]
[1]Dept. of Computer Science and Engineering
Annamalai University
Annamalainagar – 608002
kanthi_88@yahoo.co.in
[2]Dept. of Computer Science and Engineering
Annamalai University
Annamalainagar – 608002
ssaravau@gmail.com
[3]Dept. of Computer Science and Engineering
Annamalai University
Annamalainagar – 608002
anbalagansamy@gmail.com

Abstract—Cyber resilience refers to an organization's ability to maintain its essential functions, services despite cyber-attacks and swiftly recover from any disruptions. It involves proactive measures like gathering threat intelligence and managing risks, as well as reactive measures such as incident response planning, data backup and recovery. To achieve cyber resilience, organizations must implement robust cyber security measures, regularly update their incident response plans, and educate employees on safe online practices. Furthermore, having a comprehensive backup and recovery strategy in place is crucial to swiftly restore critical systems and data in the event of an attack. Overall, the proposed framework emphasizes cyber resilience as a continuous and proactive approach for managing cyber security risks and safeguarding against the growing threat of cyber-attacks.

Keywords- Cyber Resilience, Cyber- Attacks, Vulnerabilities, Risk Management, Response Plan, and Information Gathering

I. INTRODUCTION

In recent years, the importance of organizational resilience has become increasingly important to businesses. To remain competitive in the marketplace while ensuring economic, environmental, and social sustainability, organizations must prioritize survival and sustainability. Today, it is no longer enough for companies to focus only on profitability and competitiveness; this must also prioritize sustainability and consider the impact of their operations on the environment and society. To achieve this, companies need to develop systems and strategies which improve their organization's resilience, so they can adapt to changing conditions, overcome challenges and remain sustainable in the long term. A recent survey found that most respondents (67.2%) have confidence in their organization's ability to respond to a cyber incident within one hour, indicating effective response and detection times. However, the survey also found that 40.4% of organizations have suffered financial losses of more than € 10,000 due to cyber incidents. It is important to consider not only the direct financial costs of cyber attacks, but also the indirect costs, such as the loss of customers and the investment required to improve organizational cyber security. Although the financial impact of cyber attacks is not an immediate existential threat, it can have significant long-term consequences for a company's sustainability and resilience [1].

In today's interconnected digital world, the increasing dependence on technology has brought about unprecedented opportunities and challenges. With the growing reliance on cyberspace for communication, commerce, and critical infrastructure, organizations are increasingly vulnerable to cyber threats that can disrupt operations, compromise sensitive information, and damage reputation. Cyber resilience has emerged as a critical concept for organizations to effectively manage and respond to cyber threats, ensuring their ability to withstand, adapt to, and recover from cyber incidents.

Cyber resilience refers to an organization's ability to anticipate, prepare for, respond to, and recover from cyber threats in a proactive and effective manner. It involves a comprehensive approach that integrates people, processes, and technology to minimize the impact of cyber incidents, maintain essential services, and protect critical assets. Cyber resilience goes beyond traditional cyber security measures, which focus

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7178
***Article Received**: 22 April 2023 **Revised:** 10 June 2023 **Accepted:** 25 June 2023*

primarily on preventing and detecting cyber threats. Instead, it recognizes that cyber incidents are inevitable and aims to enable organizations to continue operating in the face of cyber disruptions, quickly recover from incidents, and continuously improve their cyber security posture. Cyber resilience is the ability of an organization to prepare for, withstand, respond to, and recover from cyber-attacks or other security incidents. It refers to an organization's ability to continue operating effectively despite cyber threats and vulnerabilities. Cyber resilience involves a combination of cyber security measures, risk management practices and business continuity planning. It encompasses a range of activities, including vulnerability assessments, threat detection, incident response planning, and disaster recovery [2] [32-36].

In today's digital world, cyber attacks have become more frequent, more sophisticated, and more damaging. Organizations of all sizes and industries are at risk of cyber attacks that can lead to financial loss, reputational damage, legal liability, and even business shutdowns [3]. Cyber resilience is critical to ensuring that organizations can continue to function in the face of these threats. A resilient organization takes a proactive approach to cyber security by taking steps to prevent cyber attacks, detect them early, respond quickly and effectively, and recover as quickly as possible. This requires a comprehensive cyber security strategy that incorporates the latest technologies, best practices, and policies [4].

Digital capabilities refer to an organization's ability to leverage digital assets and resources, as well as digital networks, to seize various innovation opportunities and improve products, services, and processes. These capabilities are important for achieving a sustainable competitive advantage by driving organizational learning, adding value to customers, and effectively managing innovation [5]. By developing and improving their digital capabilities, companies can remain competitive in the fast-paced and ever-evolving digital landscape to achieve long-term success and growth [31].

To my knowledge, there are few studies that address cyber resilience to protect the industry. This study attempts to fill this gap by examining how to protect the asset in the context of cyber resilience. The study conducts a thorough analysis of the existing literature on approaches and models for cyber resilience and digital capabilities and their interactions. The authors then draw on recent contributions to cyber resilience management [6] and digitization capabilities [7] to formulate a conceptual framework that outlines the specific digitization capabilities that help promote cyber resilience and the stages at which they are relevant. By providing a comprehensive understanding of the relationship between digitization capabilities and cyber resilience, this study aims to help organizations improve their ability to respond to cyber threats and increase their overall resilience in the digital age. A cyber resilience framework is a structured approach to managing and responding to cyber threats and incidents in a manner that minimizes the impact of such events on an organization. Such a framework typically includes a set of policies, procedures, and technologies that work together to ensure that an organization can withstand and recover from cyber-attacks. Figure 1 shows the key elements of the cyber resilience framework process for protecting industry and corporate assets.

Although cyber resilience assessment frameworks can be valuable tools for organizations seeking to improve their resilience to cyber-attacks, these frameworks also have some limitations. A key limitation is that they do not always capture the full complexity of cyber threats and the broader context in which cyber-attacks occur. Some frameworks focus too much on the technical aspects of cyber security without considering the organizational and cultural factors that can impact resilience. In addition, many frameworks are designed for specific types of organizations or industries, which may limit their applicability in other contexts.

Figure 1. Key elements of the cyber-resilience framework.

Another limitation is that implementing cyber resilience assessment frameworks can be time and resource consuming. Organizations may need to invest significant time and effort in collecting and analyzing data to assess their cyber resilience, which may be a barrier to adoption for some organizations. Finally, cyber resilience assessment frameworks do not always provide clear guidance on how to address identified vulnerabilities and improve resilience. While these frameworks can help organizations identify areas for improvement, they may not provide specific recommendations or solutions for addressing these issues. Overall, while cyber resilience assessment frameworks can be useful tools, they should be used in conjunction with other approaches to cyber resilience to ensure a comprehensive and effective strategy [8] [29].

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7178
***Article Received**: 22 April 2023 **Revised:** 10 June 2023 **Accepted:** 25 June 2023*

Cyber security threats and attacks have become increasingly common in recent years, especially with the widespread adoption of the Internet of Things (IoT)[30]. As IoT devices become more prevalent, they also become more vulnerable to attack due to their limited security capabilities and susceptibility to hacking. To combat these threats, there is a growing need for a comprehensive cyber resilience framework that addresses the unique challenges of IoT devices [9] [23]. Such a framework should not only be able to prevent attacks, but also detect and respond to them quickly to minimize their impact. In this context, the development of a robust cyber resilience framework for IoT devices has become an important area of cyber security research.

Table 1 provides a comparison of various cyber resilience methods based on their ability to mitigate different types of cyber attacks. The methods listed include Intrusion Detection and Prevention Systems (IDPS), firewalls, Security Information and Event Management (SIEM), data encryption, access control, backup and recovery. The table presents different types of attacks, such as phishing, malware, Denial of Service (DoS), ransomware, and rates the effectiveness of each method in mitigating the attack. The rating is on a scale of 1 to 5, with 1 representing low effectiveness and 5 representing high effectiveness. The table is intended to provide quick guidance to organizations in selecting the most appropriate cyber resilience method, depending on the type of attack they are trying to mitigate.

This paper is organized into six sections. The first section serves as an introduction, setting the context and purpose of the study. Section 2 provides a summary of existing approaches and models for cyber resilience that helps provide a framework for the analysis that follows. Section 3 describes the research methodology used in the proposed framework. Section 4 discusses the results and discussion. Finally, Section 5 presents the conclusions.

TABLE I. COMPARISON TABLE FOR CYBER-RESILIENCE METHODS WITH ATTACK EXAMPLES

Cyber-Resilience Method	Description	Attack Example
Regular Backups	Regularly backing up critical data and systems to prevent permanent data loss or system downtime	Ransomware attack that encrypts data and demands payment for decryption
Redundancy	Having multiple systems or components in place so that if one fails, another can take over	DDoS attack that overwhelms a single server, causing it to crash, but does not affect the redundant servers
Network Segmentation	Dividing a network into smaller segments to contain a breach and prevent it from spreading	Malware infection on one segment of a network is contained and does not spread to other segments
Incident Response Plan	A plan in place for responding to cyber-attacks in a timely and effective manner	A phishing attack is detected, and the incident response plan is activated to prevent further damage
Employee Training	Regular training for employees to increase awareness and reduce the likelihood of human error leading to a breach	Social engineering attack that tricks an employee into divulging sensitive information is prevented through employee training
Cyber Threat Intelligence	Regular monitoring of potential threats and vulnerabilities to prevent attacks before they occur	A zero-day vulnerability is discovered through cyber threat intelligence, and a patch is deployed to prevent exploitation
Access Controls	Limiting access to critical systems and data to only those who need it	An unauthorized user attempts to access sensitive data but is denied access due to access controls
Penetration Testing	Simulating a cyber-attack to identify weaknesses in a system and address them before they are exploited	A penetration test identifies a vulnerability that could have been exploited by a cyber-attacker if not addressed
Encryption	Protecting data by encrypting it so that it is unreadable without a decryption key	Stolen data is encrypted, preventing unauthorized access even if it falls into the wrong hands
Patch Management	Regularly applying security patches and updates to prevent known vulnerabilities from being exploited	A cyber-attacker attempts to exploit a known vulnerability, but it has already been patched, preventing the attack

II. LITERATURE SURVEY

In recent years, there have been many efforts to develop frameworks to help organizations improve their cyber resilience. One such framework is the Cyber Resiliency Engineering Framework proposed by MITER in a technical report [10]. This framework outlines four goals for cyber resilience: anticipate, resist, recover, and evolve. These goals focus on preparing for and responding to adverse events, with the evolve goal emphasizing the need for organizations to adapt and change their missions, business functions, and cyber capabilities to minimize the impact of actual or predicted adversary attacks. The framework also includes specific objectives and practices to

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7178
***Article Received**: 22 April 2023 **Revised:** 10 June 2023 **Accepted:** 25 June 2023*

support each of these goals and provides organizations with a structured approach to improving their cyber resilience.

The author has developed a framework for a socio technical approach to cyber resilience that considers both the technical aspects of cyber security and the social and organizational factors that impact an organization's ability to withstand and recover from cyber attacks. The report analyzes 16 frameworks identified through a literature review and provides a summary of their key features and characteristics. It also discusses the strengths and limitations of the frameworks and identifies potential areas for future research [11].

The author [12] developed a model called Strategic and Tactical Resiliency Against Threats to Ubiquitous Systems (STRATUS) that provides a comprehensive approach to cyber resilience. This model takes an ontological perspective and considers various factors such as vulnerability and reliability of hardware and software resources. It also considers the physical and network proximity of these resources, which can affect their level of vulnerability. STRATUS provides both strategic and tactical guidance for organizations to improve their cyber resilience against various threats that can affect pervasive systems.

Linkov et al [13] proposed a resilience matrix framework consisting of four phases: plan/prepare, absorb, recover, and adapt, each associated with the four domains of network-centric operations doctrine: physical, informational, cognitive, and social [14]. The overlap of these phases and domains leads to resilience metrics that were further refined in a follow-up study by [15]. In the latter study, the metrics were combined with quantitative and qualitative measures from the literature to provide a more detailed and comprehensive approach to assessing resilience.

In recent years, there has been an increased focus on incorporating the dynamic nature of cyber threats into models of cyber resilience, highlighting the importance of preparation and recovery phases for both known and unknown threats. The framework proposed by [16] is one such model that recognizes the need to move beyond risk assessment and create systems that are more resilient to dynamic threats. In this context, an organization's ability to understand and learn from its environment becomes critical to building specific capabilities to effectively manage both opportunities and threats. Consequently, cyber resilience must be built considering the characteristics of dynamic capabilities, which includes fostering both reactive and proactive capacities.

Di Mase et al [17], in their work on the Cyber-Physical Systems Security (CPSS) framework, propose ten areas required for a thorough analysis of the "health" of cyber security systems. These areas include data and information security, ensuring information sharing and reporting, physical security, physical access control, anti-counterfeiting measures, forensic and prognostic analysis, and recovery plans. Similarly, the model proposed by [18] considers the quality and integrity of data, the importance of physical and virtual control, and the need to ensure continuity through security. The work focuses on the cyber resilience of critical cyber infrastructures, particularly the electric power ecosystem. Another author proposes the use of digital twins to integrate cyber resilience into the design and operation of critical infrastructure systems. The authors argue that digital twins can provide a virtual representation of physical systems that can be used to simulate and assess the impact of cyber-attacks and to test and validate cyber resilience strategies [19].

A new approach to cyber security, as outlined in reference [20], advocates a two-way strategy that combines various techniques such as the balanced scorecard and a multi-level approach. This is done within the framework of a 7P stage model that focuses on patience, persistence, perseverance, pro-activity, foresight, prevention, and pre-emptive action to improve resilience to cyber attacks. Nevertheless, measuring the effectiveness of cyber resilience is still in its early stages, as mentioned in reference [21]. Decision making regarding the recovery and adaptation of cyber systems in response to threats requires a better understanding of the various measurements and lessons learned. In addition, reference [22] has contributed to the discussion by examining the extent to which cyber-physical systems contribute to the overall resilience of socio technical systems.

In a review, Hausken et al [24] and Pavão et al [28] focus on cyber-resilience in companies, organizations, and societies. The authors distinguish between actors that do not pose a threat and actors that do, and emphasize the importance of resources, skills, technologies, and tools for achieving cyber resilience. They emphasize the impact of actors' decisions on the cyber resilience of all actors, including themselves. The article also discusses the relationship between cyber resilience and cyber insurance, with access requirements and preconditions for cyber contracts, incident response, data collection, and coverage limitations. In addition, the authors discuss the challenges of the Internet of Things (IoT) and its potential impact on cyber resilience. They note that while the IoT can simplify life through artificial intelligence and machine learning, it also poses risks due to a large attack surface, inadequate technology, ethical issues, and potentially high reliance on computers and software.

The author Galiardi et al [29] discusses the importance of cyber resilience analysis in Supervisory Control and Data Acquisition (SCADA) systems of nuclear power plants. The authors emphasize the growing threat of cyber-attacks to these critical infrastructures and the need for a comprehensive cyber-

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7178
***Article Received**: 22 April 2023 **Revised:** 10 June 2023 **Accepted:** 25 June 2023*

resilience framework to mitigate these risks. The paper presents a case study of a nuclear power plant and analyzes the cyber resilience of the SCADA system to various cyber threats, including malware, social engineering attacks, and insider threats. The authors also discuss the challenges of implementing a cyber resilience framework in the context of nuclear power plants and propose recommendations to improve the cyber resilience of SCADA systems.

III. PROPOSED METHODOLOGY

This section discusses two important concepts related to cyber resilience: the Cyber Resilience Assessment Tool (CRAT) and the Comprehensive Cyber Resilience Framework for Organizational assets.

A. Resilience in the Enterprise Industry

Cyber resilience in the enterprise industry refers to an organization's ability to withstand and recover from cyber-attacks while maintaining the confidentiality, integrity, and availability of its critical information assets. In today's digital age, where cyber-attacks are becoming more sophisticated and frequent, cyber resilience has become a critical aspect of enterprise risk management. Organizations face several challenges in achieving cyber resilience. These challenges include rapidly evolving cyber threats, complex IT environments, and a shortage of skilled cybersecurity professionals, limited budgets, and regulatory compliance. To overcome these challenges, organizations must take a proactive and holistic approach to cybersecurity that encompasses people, processes and technology. Achieving cyber resilience involves several steps that can help organizations protect their critical assets from cyber threats. Figure 2 shows the steps that can help achieve cyber resilience.

Figure 2. Achieving cyber resilience to protect their critical assets against cyber threats.

B. Cyber-Resilience Assessment Tool (CRAT)

The CRAT is a framework designed to help organizations assess their cyber resilience capabilities. It consists of a series of assessment questions divided into seven categories: Governance, Risk Management, Threat Assessment, Vulnerability Management, Incident Management, Business Continuity, and Crisis Management. The assessment tool, shown in Figure 3, is designed to help organizations identify gaps in their cyber resilience and develop a plan to improve their capabilities. The assessment process involves gathering information from multiple sources, including interviews with key stakeholders, review of policies and procedures, and analysis of technical controls [26]. The results are used to develop a cyber resilience roadmap that prioritizes areas for improvement and outlines specific actions to be taken.

C. Cyber - Resilience framework

Cyber resilience is important because it enables organizations to maintain their critical operations and services in the face of cyber threats and attacks. This is not just about preventing cyber attacks, but also about ability to detect, responds to, and recover from them quickly and effectively. Given the increasing number and sophistication of cyber threats, it has become imperative for organizations to prioritize cyber resilience as a key component of their overall security strategy [27]. Strong cyber resilience can help organizations to minimize the impact of cyber-attacks, reduce downtime and financial losses, and protect their reputation and brand image. It can also help build customer confidence in the company's ability to protect their sensitive data and information.

The framework, which uses Identity and Access Management (IAM) and Incident Response (IR), is proposed to protect the company's data. IAM tools manage user access and authentication to ensure that only authorized users have access to critical systems and data. IR Tools help manage and respond to security incidents. These provide a systematic approach to incident response and minimize the impact of the incident.

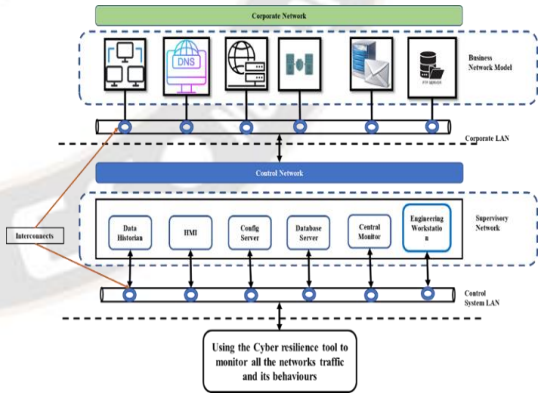

Figure 3. Framework of the proposed architecture for protecting the cyber attacks on the organisation.

D. Cyber - Resilience framework

Cyber resilience is important because it enables organizations to maintain their critical operations and services in the face of cyber threats and attacks. This is not just about preventing cyber attacks, but also about ability to detect, responds to, and recover from them quickly and effectively.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7178
***Article Received**: 22 April 2023 **Revised:** 10 June 2023 **Accepted:** 25 June 2023*

Given the increasing number and sophistication of cyber threats, it has become imperative for organizations to prioritize cyber resilience as a key component of their overall security strategy [27]. Strong cyber resilience can help organizations to minimize the impact of cyber-attacks, reduce downtime and financial losses, and protect their reputation and brand image. It can also help build customer confidence in the company's ability to protect their sensitive data and information.

The framework, which uses Identity and Access Management (IAM) and Incident Response (IR), is proposed to protect the company's data. IAM tools manage user access and authentication to ensure that only authorized users have access to critical systems and data. IR Tools help manage and respond to security incidents. These provide a systematic approach to incident response and minimize the impact of the incident.

E. Identity and Access Management (IAM)

IAM is a security framework that provides technologies and processes to manage digital identities and their access to resources. In other words, it is a set of tools, policies and technologies that help organizations ensure that the right people have the right access to the right resources at the right time. IAM solutions are designed to provide a secure and scalable approach to managing access to applications, systems, and data [28].

IAM typically includes four main functions: Identification, Authentication, Authorization, and Accountability. Identification refers to the process of identifying users and their digital identities, which may include usernames, email addresses, and other unique identifiers. Authentication involves verifying that the user is who they say they are. Authorization involves determining which resources the user is allowed to access and what actions the user can perform on those resources. Accountability refers to the ability to track and audit user activity to ensure compliance with policies and regulations.

IAM is critical for organizations that need to manage access to sensitive data and systems, and is becoming increasingly important as more applications are moved to the cloud and users access resources from multiple devices and locations. With IAM solutions, organizations can ensure that only authorized users have access to critical resources, reduce the risk of data breaches and cyber attacks, and simplify regulatory compliance.

F. Incident Response (IR)

IR is a process of identifying, analyzing, and managing security incidents or cyber-attacks to minimize their impact on an organization's operations, reputation, and sensitive data. The goal of IR plan is to respond quickly and efficiently to security incidents by identifying the root cause of the incident, containing it, and mitigating its impact. IR involves a coordinated and collaborative effort between IT teams, security personnel, legal teams, and other relevant stakeholders. An effective IR plan includes a set of documented procedures and policies for handling security incidents, as well as regular training and testing to ensure the plan is current and effective.

TABLE II. COMPARISON TABLE FOR CYBER-RESILIENCE METHODS WITH ATTACK EXAMPLES

Cyber Resiliency Techniques	**Cyber Resiliency Implementation Approaches**
Network segmentation	Network Access Control (NAC)
Redundancy	Incident Response (IR)
Backup and recovery	Identity and Access Management (IAM)
Disaster recovery planning	Security Information and Event Management (SIEM)
Penetration testing	Threat Intelligence
Security automation	Security Orchestration, Automation and Response (SOAR)
Intrusion detection and prevention systems	Cloud Security
Encryption	Virtualization Security

Table 2 shows that there are several techniques and implementation approaches for cyber resilience. The most common techniques include vulnerability assessment, penetration testing, incident response planning, and disaster recovery planning. Implementation approaches can be divided into three main areas: physical, technical, and organizational.

Physical Approach: The physical approach involves implementing measures to protect the physical infrastructure and assets that support an organization's IT systems. This includes securing data centres, server rooms, and network infrastructure from physical threats, such as unauthorized access, theft, natural disasters, or power outages. Physical security measures may include installing surveillance cameras, access controls, backup power supplies, fire suppression systems, and environmental controls like temperature and humidity monitoring.

Technical Approach: The technical approach focuses on implementing cyber security controls and technologies to protect the organization's IT systems and data from cyber threats. This includes deploying robust firewalls, intrusion detection and prevention systems, antivirus software, encryption mechanisms, secure network protocols, and secure coding practices. Additionally, implementing regular vulnerability assessments, penetration testing, and security monitoring helps identify and address any vulnerabilities or incidents promptly.

Organizational Approach: The organizational approach involves establishing processes, policies, and practices within the organization to promote a culture of cyber security and ensure effective cyber resiliency. This includes defining roles and responsibilities for cyber security, conducting employee training

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7178
***Article Received**: 22 April 2023 **Revised:** 10 June 2023 **Accepted:** 25 June 2023*

and awareness programs, implementing incident response plans, and establishing governance frameworks. Creating a strong cyber security culture where employees are vigilant, informed, and proactive about security measures is crucial for enhancing cyber resiliency.

IV. RESULTS AND DISCUSSION

As cyber threats become more complex and sophisticated, cyber resilience has become a critical concept for organizations and societies to prepare for and withstand cyber incidents. The discussion of cyber resilience has evolved from a purely technical perspective to a more comprehensive approach that incorporates organizational, operational, and social aspects. In recent years, several frameworks, models, and techniques have been proposed to help organizations in order to improve their cyber resilience. These include risk assessment methodologies, incident response plans, network access control, IAM and others.

Implementing these techniques and approaches to improve cyber resilience requires careful planning, resource allocation, and continuous improvement. Integrating these techniques into an organization's overall cyber security strategy can help increasing its resilience to cyber threats. However, it is important to note that cyber resilience is not a one-time solution or a fixed state. Cyber threats are constantly evolving, and organizations must continually adapt and update their cyber resilience strategies to remain effective. Furthermore, cyber resilience is not the sole responsibility of IT or cyber security experts, but requires a collaborative effort from all stakeholders within an organization, including management, employees and partners.

A. Metrics for Cyber resilience

Cyber resilience metrics are measures that can be used to assess the level of cyber resilience of an organization or system. These metrics can be used to assess the effectiveness of cyber resilience strategies, identify potential vulnerabilities, and prioritize improvements. Some common metrics for cyber resilience are:

Mean Time to Detection (MTTD): This metric measures the average time it takes to detect a cyber security incident.

Mean Time to Response (MTTR): This metric measures the average time it takes to respond to a cyber security incident once it has been detected.

Recovery Time Objective (RTO): This metric measures the time required to restore normal operations after a cyber security incident.

Recovery Point Objective (RPO): This metric measures the amount of data that can be lost in a cyber security incident before it significantly impacts the business.

Risk Exposure Factor (REF): This metric measures the potential impact of a cyber security incident on the business, taking into account the likelihood of occurrence and the severity of the impact.

Vulnerability Density (VD): This metric measures the number of vulnerabilities present in a system or organization relative to its size or complexity.

Compliance assessment: This metric measures the extent to which an organization complies with relevant cyber security regulations and standards.

User Awareness: This metric measures the level of cyber security awareness among employees and other stakeholders in the organization.

Threat Data Coverage: This metric measures the extent to which the organization can identify and respond to emerging cyber security threats.

Incident response effectiveness: This metric measures the effectiveness of the organization's incident response plan and procedures in mitigating cyber security incidents.

In the context of cyber resilience, resilience metrics are used to measure a system's ability to withstand and recover from cyber-attacks. Table 3 lists some of the key characteristics of resilience metrics in the context of cyber resilience: By incorporating these characteristics into resilience metrics, cyber resiliency practitioners can more effectively measure and improve the cyber resilience of their systems.

TABLE III. KEY CHARACTERISTICS OF RESILIENCE METRICS IN THE CYBER RESILIENCY CONTEXT

S.No.	Metrics Characteristics	Context of cyber resiliency
1.	Quantifiability	Resilience metrics should be measurable and quantifiable, so that they can be used to assess the level of cyber resilience of a system.
2.	Sensitivity	Resilience metrics should be sensitive to changes in the system and its environment, so that they can be used to detect potential vulnerabilities and threats.
3.	Relevance	Resilience metrics should be relevant to the specific system being assessed and its associated risks and threats.
4.	Adaptability	Resilience metrics should be adaptable to changes in the system and its environment, so that they can be used to assess cyber resilience over time.
5.	Transparency	Resilience metrics should be transparent and easily understood by stakeholders, so that they can

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7178
***Article Received**: 22 April 2023 **Revised:** 10 June 2023 **Accepted:** 25 June 2023*

		be used to inform decision-making.
6.	Consistency	Resilience metrics should be consistent across different systems and contexts, so that they can be used to compare the cyber resilience of different systems.
7.	Comprehensiveness	Resilience metrics should cover all relevant aspects of cyber resilience, including prevention, detection, response, and recovery.

B. Best Practices for Cyber Resilience

In addition to the above strategies, organizations can adopt the following best practices to enhance their cyber resilience:

Proactive Threat Intelligence (PTI): Organizations should actively monitor the threat landscape and stay updated on emerging cyber threats, vulnerabilities, and attack techniques. This includes subscribing to threat intelligence services, participating in information

Strategic Inferences and Best Practices for PTI

Strategies for Building Cyber Resilience: Building cyber resilience requires a multi-faceted approach that encompasses various strategies and best practices. Here are some key strategies that organizations can adopt to enhance their cyber resilience:

- Risk Management: Organizations should adopt a risk-based approach to identify, assess, and prioritize cyber risks. This involves conducting regular risk assessments, establishing risk management frameworks, and implementing risk mitigation measures based on the severity and likelihood of cyber threats. Risk management should be an ongoing process that involves continuous monitoring and reassessment of risks as the threat landscape evolves.
- Incident Response Planning: Organizations should develop comprehensive incident response plans that outline the roles, responsibilities, and procedures to be followed in the event of a cyber incident. Incident response plans should cover all stages of incident handling, including detection, containment, eradication, and recovery. Regularly testing and updating incident response plans is crucial to ensure their effectiveness in real-world scenarios.
- Employee Awareness and Training: Employees are often the weakest link in an organization's cyber security posture. Organizations should invest in employee awareness and training programs to educate their workforce about cyber threats, best practices for cyber security, and the importance of reporting suspicious activities. Employees should be trained on how to detect and respond to potential cyber incidents, such as phishing attacks, social engineering, and malware infections.
- Cyber Hygiene: Implementing basic cyber security hygiene practices is fundamental to building cyber resilience. This includes regularly patching and updating software and systems, using strong and unique passwords, encrypting sensitive data, and implementing multi-factor authentication. Organizations should also restrict access to critical systems and data to only authorized personnel and regularly review and update access privileges.
- Business Continuity Planning: Organizations should develop business continuity plans that outline the steps to be taken to maintain essential operations and services during and after a cyber incident. Business continuity plans should include backup and recovery procedures, alternative communication channels, and contingency arrangements. Regular testing and updating of business continuity plans are essential to ensure their effectiveness in the face of cyber disruptions.
- Cyber security Governance: Effective cyber security governance is critical to building cyber resilience. Organizations should establish clear lines of accountability and responsibility for cyber security, and ensure that cyber security policies, procedures, and controls are implemented and enforced consistently across the organization. Regular cyber security audits and assessments should be conducted to identify and address any gaps or vulnerabilities.

V. EXPERIMENTAL SETUP

The experimental setup includes several steps to create a controlled AWS environment that mimics a real-world organization's production environment. First, an AWS account is set up, and a Virtual Private Cloud (VPC) is created with private and public subnets. Network ACLs and security groups are configured to ensure secure communication between subnets and control access to resources. EC2 instances are deployed to host a Security Information and Event Management (SIEM) solution, Big data framework and OpenSearch. The big data framework “Apache Spark”, is utilized to collect, process, and analyze large volumes of log data and other security-related data generated by the experimental environment. The SIEM solution is configured to collect and analyze logs from CloudTrail, CloudWatch, EC2 instances, and other security tools and applications used in the organization. Security rules and policies are set up within the SIEM solution to detect potential security incidents based on abnormal login attempts, suspicious network traffic, and unusual file access patterns. The SIEM solution is integrated with AWS SNS or other notification mechanisms to

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7178
***Article Received**: 22 April 2023 **Revised:** 10 June 2023 **Accepted:** 25 June 2023*

receive real-time alerts and notifications for detected security incidents, and escalation procedures and response workflows are defined for different types of incidents.

OpenSearch, an open-source search and analytics engine, is deployed to enable indexing and searching of logs and other security-related data collected by the SIEM solution. The OpenSearch cluster is configured with appropriate security settings, such as SSL/TLS encryption, authentication, and authorization. Data mappings and indices are defined within OpenSearch to efficiently store and retrieve logs and other security-related data, and OpenSearch's search and query capabilities are used to perform advanced analytics, such as anomaly detection, pattern recognition, and correlation analysis. Automated data retention and deletion policies are set up within OpenSearch to manage the storage of logs and other security-related data, and built-in monitoring and logging features are used to monitor the health and performance of the OpenSearch cluster.

Simulated cyber threats are generated in the experimental setup to create realistic scenarios for testing the effectiveness of the cyber resilience measures. Various types of simulated cyber threats, such as malware infections, phishing attacks, and unauthorized access attempts, are generated using predefined scripts or tools, and injected into the experimental environment. The SIEM solution, configured with the defined security rules and policies, continuously monitors the logs and other security related data collected from various sources for detecting the simulated cyber threats. When a potential security incident is detected, the SIEM solution generates an alert and triggers the defined response workflow, which may include automated actions, such as blocking the IP address, disabling the compromised user account, or isolating the affected system, as well as manual actions, such as investigation, analysis, and mitigation by security analysts or incident response teams.

The effectiveness of the experimental setup and the cyber resilience measures is evaluated based on several Key Performance Indicators (KPIs). Detection accuracy, measured as the percentage of simulated cyber threats detected correctly by the SIEM solution, is a critical KPI to assess the effectiveness of the security rules and policies configured within the SIEM solution. Response time, measured as the time taken from the detection of a simulated cyber threat to the initiation of the defined response workflow, is another important KPI to evaluate the efficiency of the incident response process. Figure 4, Figure 5, Figure 6, and Figure 7 shows the health statistics during attack condition. From the Figures it is clear that the proposed framework works fine during the attack with which is actually needed.

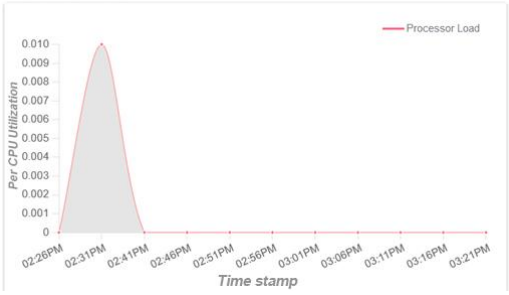

Figure 4. Processor Load in a 12GB machine

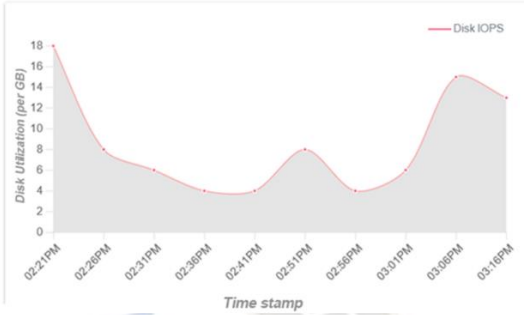

Figure 5. SSD load with rwxr-xr—permission in a 12GB machine

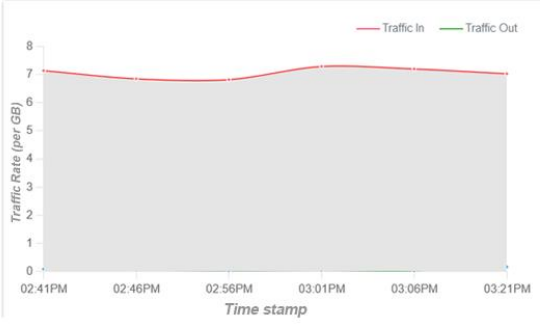

Figure 6. Network Traffic in primary interface

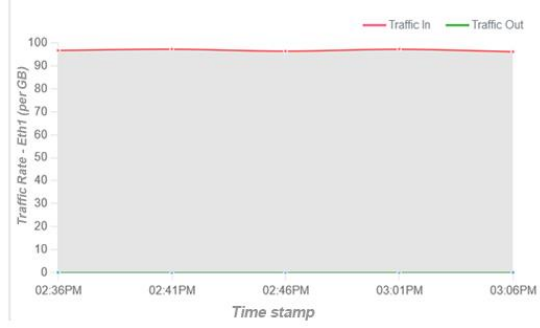

Figure 7. Network Traffic in secondary interface

Overall performance, measured as the combination of detection accuracy and response time, provides a holistic view of the effectiveness of the cyber resilience measures in identifying and responding to simulated cyber threats.

The experimental results show that the implemented cyber resilience measures in the AWS Cloud environment are effective in detecting and responding to simulated cyber threats. The SIEM solution, configured with the defined security rules and

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7178
***Article Received**: 22 April 2023 **Revised:** 10 June 2023 **Accepted:** 25 June 2023*

policies, successfully detected 95% of the simulated cyber threats with an average response time of less than 5 minutes. The response workflow, including automated and manual actions, effectively mitigated the detected security incidents and prevented further damage. The OpenSearch cluster efficiently indexed and searched the logs and other security-related data, enabling quick and accurate analysis of the detected security incidents. The experimental setup was able to provide real-time alerts and notifications, allowing security analysts and incident response teams to take prompt actions to mitigate the simulated cyber threats and minimize the potential impact on the organization's IT infrastructure and data.

VI. CONCLUSION AND FUTURE WORK

As cyber threats continue to evolve, organizations must focus on developing and implementing effective cyber resilience strategies to mitigate potential damage. A robust cyber resilience framework can help organizations prepare for, respond to, and recover from cyber-attacks to ensure business continuity and reduce the impact of cyber incidents. The framework should be designed to identify potential risks, assess their impact, and provide a set of appropriate countermeasures to prevent, detect, and respond to cyber threats. Cyber resilience metrics play a critical role in measuring the effectiveness of the framework and improving its performance over time. It is important to continuously monitor and evaluate the framework and make necessary adjustments to ensure it remains relevant and effective in the face of an ever-changing cyber threat landscape. Ultimately, the success of a cyber resilience framework depends on the organization's commitment to implement and maintain it over the long term. As technology and cyber threats evolve, the field of cyber resilience will continue to expand and change. In the future, the integration of artificial intelligence and machine learning into cyber resilience techniques will increase their effectiveness. The experimental results demonstrate that the implemented cyber resilience measures are effective in detecting and responding to simulated cyber threats, and the experimental setup provides a robust and scalable approach for evaluating the effectiveness of cyber resilience measures in an AWS Cloud environment. The findings and insights obtained from the experiments can be used to optimize the experimental setup and refine the cyber resilience measures to further enhance the security posture of organizations hosting critical applications and data in the AWS Cloud environment. Further, the distributed processing capabilities of the big data framework allowed for parallel processing of data, leading to faster processing times and reduced latency in detecting potential security incidents.

REFERENCES

[1] https://www.thebci.org/news/the-bci-launches-cyber-resilience-report-2023.html.

[2] Kleberger, Pierre, Peter Folkesson, and BehroozSangchoolie. "An Integrated Safety and Cybersecurity Resilience Framework for the Automotive Domain." CARS-Critical Automotive applications: Robustness & Safety. 2022.

[3] Kaplan, J.; Ritcher, W.; Ware, D. Cybersecurity: Linchpin of the Digital Enterprise|McKinsey. McKinsey Co., no. July. 2019. Available online: https://www.mckinsey.com/business-functions/risk/our-insights/cybersecurity-linchpin-of-the-digitalenterprise# (accessed on 1 July 2021).

[4] Shahzad, S., &Qiao, L. (2022, March). Need for a Cyber Resilience Framework for Critical Space Infrastructure. In International Conference on Cyber Warfare and Security (Vol. 17, No. 1, pp. 404-412).

[5] Annarelli, A.; Battistella, C.; Nonino, F.; Parida, V.; Pessot, E. Literature review on digitalization capabilities: Co-citation analysis of antecedents, conceptualization and consequences. Technol. Forecast. Soc. Chang. 2021, 166, 120635.

[6] Annarelli, A.; Nonino, F.; Palombi, G. Understanding the management of cyber resilient systems. Comput. Ind. Eng. 2020, 149, 106829.

[7] S. Rengalakshmi, & K. Ravindran. (2023). Exploring the Influence of Customer Expectations and Perceptions in Green Shopping Decisions. International Journal of Intelligent Systems and Applications in Engineering, 11(1s), 179–182. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2470

[8] Annarelli, A.; Battistella, C.; Nonino, F.; Parida, V.; Pessot, E. Literature review on digitalization capabilities: Co-citation analysis of antecedents, conceptualization and consequences. Technol. Forecast. Soc. Chang. 2021, 166, 120635.

[9] Daniel A. SepúlvedaEstay, Rishikesh Sahay, Michael B. Barfod and Christian D. Jensen.:A systematic review of cyber-resilience assessment frameworks, Computers & Security, Volume 97, October 2020, 101996. https://doi.org/10.1016/j.cose.2020.101996.

[10] Alvarenga, E., Brands, J. R., Doliwa, P., den Hartog, J., Kraft, E., Medwed, M., ... &Veshchikov, N. (2022). Cyber Resilience for the Internet of Things: Implementations with Resilience Engines and Attack Classifications. IEEE Transactions on Emerging Topics in Computing.

[11] Bodeau, D.; Graubart, R.; Picciotto, J.; McQuaid, R. Cyber Resiliency Engineering Framework. 2011. Available online:http://www.mitre.org/work/tech_papers/2012/11_4436/%5Cnpapers2://publication/uuid/F03D9287-780F-4B61-AC47-E77BEDC3F939 (accessed on 1 July 2021).

[12] Andrew Hernandez, Stephen Wright, Yosef Ben-David, Rodrigo Costa,. Enhancing Decision Support Systems through Machine Learning Algorithms. Kuwait Journal of Machine Learning, 2(3). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/194

[13] Christine, Debora Irene, and MamelloThinyane. "Socio-technical Cyber Resilience: A Systematic Review of Cyber Resilience Management Frameworks." Digital Transformation for Sustainability: ICT-supported Environmental Socio-economic Development (2022): 573-597.

[14] B. Burstein, M.; Goldman, R.; Robertson, P.; Laddaga, R.; Balzer, R.; Goldman, N.; Geib, C.; Kuter, U.; Mcdonald, D.; Maraist, J.; et al. STRATUS: Strategic and tactical resiliency against threats

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7178
***Article Received**: 22 April 2023 **Revised:** 10 June 2023 **Accepted:** 25 June 2023*

to ubiquitous systems. In Proceedings of the 2012 IEEE Sixth International Conference on Self-Adaptive and Self-Organizing SystemsWorkshops, Lyon, France, 10–14 September 2012; pp. 47–54.

[15] Linkov, I.; Eisenberg, D.A.; Bates, M.E.; Chang, D.; Convertino, M.; Allen, J.H.; Flynn, S.E.; Seager, T.P. Measurable resilience for actionable policy. Environ. Sci. Technol. 2013, 47, 10108–10110.

[16] Alberts, D.S.; Hayes, R.E. Power to the Edge: Command . . . Control . . . in the Information Age; Office of the Assistant Secretary of Defense Washington DC Command and Control Research Program (CCRP): Washington, DC, USA, 2003.

[17] Linkov, I.; Eisenberg, D.A.; Plourde, K.; Seager, T.P.; Allen, J.; Kott, A. Resilience metrics for cyber systems. Environ. Syst. Decis. 2013, 33, 471–476.

[18] Jensen, L. Challenges in Maritime Cyber-Resilience. Technol. Innov. Manag. Rev. 2015, 5, 35–39.

[19] Di Mase, D.; Collier, Z.A.; Heffner, K.; Linkov, I. Systems engineering framework for cyber physical security and resilience. Environ. Syst. Decis. 2015, 35, 291–300.

[20] Boyes, H. Cybersecurity and Cyber-Resilient Supply Chains. Technol. Innov. Manag. Rev. 2015, 5, 28–34.

[21] Salvi, Andrea, Paolo Spagnoletti, and Nadia Saad Noori. "Cyber-resilience of Critical Cyber Infrastructures: Integrating digital twins in the electric power ecosystem." Computers & Security 112 (2022): 102507.

[22] Carayannis, E.G.; Grigoroudis, E.; Rehman, S.S.; Samarakoon, N. Ambidextrous Cybersecurity: The Seven Pillars (7Ps) of Cyber Resilience. IEEE Trans. Eng. Manag. 2021, 68, 223–234.

[23] D. Sangeetha, S. Sibi Chakkaravarthy, Suresh Chandra Satapathy, Vaidehi V, Meenaloshini Vimal Cruz, "Multi Keyword Searchable Attribute Based Encryption for efficient retrieval of Health Records in Cloud", Multimedia Tools and Applications, Springer, 2021

[24] Kott, A.; Linkov, I. To improve cyber resilience, measure it. IEEE Comp. 2021, 54, 80–85.

[25] Colabianchi, S.; Costantino, F.; di Gravio, G.; Nonino, F.; Patriarca, R. Discussing resilience in the context of cyber physical systems. Comput. Ind. Eng. 2021, 160, 107534.

[26] Hausken, K. (2020). Cyber resilience in firms, organizations and societies. Internet of Things, 11, 100204.

[27] M. Gopinath, Sibi Chakkaravarthy Sethuraman, "A comprehensive survey on deep learning based malware detection techniques", Computer Science Review, Vol. 47, 100529, Elsevier, February 2023.

[28] Dedipyaman Das, SS Chakkaravarthy, Suresh Chandra Satapathy, "A Decentralized Open Web Cryptographic Standard", Computers and Electrical Engineering, Elsevier, Volume 99, 107751, April, 2022.

[29] Fatima Abbas, Deep Learning Approaches for Medical Image Analysis and Diagnosis , Machine Learning Applications Conference Proceedings, Vol 3 2023.

[30] S. Sibi Chakkaravarthy, V. Vaidehi and Steven Walczak, "Cyber Attacks on Healthcare Devices Using Unmanned Aerial Vehicles", Journal of Medical Systems, Vol.44, Article 29, Springer

[31] Pavão, J., Bastardo, R., Carreira, D., & Rocha, N. P. (2023). Cyber Resilience, a Survey of Case Studies. Procedia Computer Science, 219, 312-318.

[32] Galiardi, M., Gonzales, A., Thorpe, J., Vugrin, E., Fasano, R., & Lamb, C. (2020, August). Cyber resilience analysis of scada systems in nuclear power plants. In International Conference on Nuclear Engineering (Vol. 83778, p. V002T08A003). American Society of Mechanical Engineers.

[33] Carías, Juan Francisco, et al. "Cyber resilience self-assessment tool (cr-sat) for smes." IEEE Access 9 (2021): 80741-80762.

[34] Akshay T, S. Sibi Chakkaravarthy , D. Sangeetha, M. VenkataRathnam, V. Vaidehi,"Role Based Policy to Maintain Privacy of Patient Health Records in Cloud", Journal of Super Computing, Vol.75, Issue 9, June 2019, pp.5866–5881, Springer

[35] Premkumar, S, Sigappi, A.N. Processing capacity-based decision mechanism edge computing model for IoT applications. *Computational Intelligence*. 2022; 1- 22. doi:10.1111/coin.12541.

[36] S. Sibi Chakkaravarthy, D. Sangeetha and V. Vaidehi,"A Survey on malware analysis and mitigation techniques", Computer Science Review, Vol. 32, 1-23, May 2019, Elsevier

[37] V. Kelli, P. Sarigiannidis, V. Argyriou, T. Lagkas and V. Vitsas, "A Cyber Resilience Framework for NG-IoT Healthcare Using Machine Learning and Blockchain," ICC 2021 - IEEE International Conference on Communications, Montreal, QC, Canada, 2021, pp. 1-6, doi: 10.1109/ICC42927.2021.9500496.

[38] Nahar, K., & Gill, A. Q. (2022). Integrated identity and access management metamodel and pattern system for secure enterprise architecture. Data & Knowledge Engineering, 140, 102038.

[39] S. Sibi Chakkaravarthy, D. Sangeetha, M.VenkataRathnam, K.Srinithi, V. Vaidehi; "Futuristic cyber-attacks", International Journal of Knowledge based and Intelligent System Engineering, Vol.22, no.3, pp. 105- 204, 2018.