Proposed Cybersecurity Framework for Reducing The Security Risks On The Egyptian Petroleum Sector

Adham Badran [(1)] ,**Sayed AbdelGaber** [(2)], **Riham Haggag** [(3)]

Abstract

Many firms are going through a digital transformation because of various issues with their operating systems, applications, and information networks. This is especially true for those in the petroleum industry. Consequently, these entities are at a higher risk of being subjected to cyberattacks, including but not limited to network, application, cloud, Internet of Things, a virtual local area network (VLAN), and software-defined networking (SDN) threats. Consequently, these attacks affected the company's ability to protect its assets, make money, gain the trust of customers, maintain its reputation, and effectively and efficiently carry out its goal. Cyberattacks could target the petroleum industry and its associated systems, such as the Supervisory control and data acquisition (SCADA) System.

The proposed framework is highlighted the importance of developing a comprehensive cybersecurity framework to reduce security threats faced by organizations, particularly in the petroleum sector, aiding strategic planning and tactical demands. Adopting a cybersecurity framework helps

[1] PhD researcher, Department of Business Information Systems, Faculty of Commerce and Business Administration, Helwan University.

[2] Professor of Information System, Faculty of Computers and Artificial Intelligence, Helwan University.

[3] Dr. in Business information Systems Department, Faculty of Commerce and Business Administration, Helwan University.

organizations manage IT risks internally, mature internal controls, and effectively manage risks across organizations.

This research is Presented 22 domains, 5 functions, and 301 controls as a part of the suggested framework.

The suggested cybersecurity framework will assist the organizations' assets from security risks in the petroleum industry, both generally and specifically in Egypt, as well as their reputation and capacity to carry out their missions completely and successfully. It is suggested applying this framework to other industries to multiply the benefits.

Keywords: Cybersecurity Framework, Reducing Security Risks, Petroleum Sector

إطار أمنى سيبرانى مقترح للحد من المخاطر الأمنية بقطاع البترول المصرى

الملخص

أدى التحول الرقمى الذى تمر به العديد من الشركات إلى حدوث العديد من المشكلات المختلفة والتى تتعلق بأنظمة التشغيل والتطبيقات وشبكات المعلومات الخاصة بها، وهذا ينطبق بشكل خاص على صناعة النفط مما يجعلها معرضة بشكل أكبر لخطر التعرض للهجمات الإلكترونية، بما في ذلك على سبيل المثال لا الحصر، لتهديدات الشبكة والتطبيقات والحوسبة السحابية وإنترنت الأشياء والشبكة المحلية الافتراضية (VLAN) والشبكات المعرفة بالبرمجيات(SDN) .

أثرت هذه الهجمات على قدرة الشركة على حماية أصولها وجني الأموال وكسب ثقة العملاء والحفاظ على سمعتها وتنفيذ أهدافها بفعالية وكفاءة. يمكن أن تستهدف الهجمات الإلكترونية صناعة النفط والأنظمة المرتبطة بها، مثل نظام التحكم الإشرافي والحصول على البيانات (SCADA). ويبين الإطار المقترح للأمن السيبراني كيفية الحد من التهديدات الأمنية التي تواجهها المنظمات، وخاصة في قطاع النفط، مما يساعد في التخطيط الاستراتيجي والمتطلبات التكتيكية. ويساعد اعتماد إطار عمل للأمن السيبراني المؤسسات على إدارة مخاطر تكنولوجيا المعلومات داخليًا، والضوابط الداخلية الناضجة، وإدارة المخاطر بشكل فعال عبر المؤسسات. تم تقديم إطار أمنى سيبرانى مقترح يتكون من 22 مجالًا و5 وظائف و301 عنصر تحكم، ويفترض أن هذا الإطار المقترح سيساعد في حماية أصول المنظمات من المخاطر الأمنية في صناعة البترول بشكل عام وفى مصر بشكل خاص، بالإضافة إلى الحفاظ على سمعتها وقدرتها على تنفيذ مهامها بشكل كامل وناجح، ومن ثم تقترح تلك الورقة البحثية تطبيق هذا الإطار المقترح على الصناعات الأخرى لمضاعفة الفوائد.

الكلمات المفتاحية: إطار أمنى سيبرانى، الحد من المخاطر الأمنية، قطاع البترول

1. Introduction

Many organizations—particularly those in the petroleum industry—are undergoing a digital transformation due to numerous flaws in their information networks, operating systems, and applications. As a result, these organizations are more vulnerable to electronic attacks, which take the form of network attacks, application attacks, cloud attacks, Internet of Things attacks, VLAN attacks, and SDN attackers. As a result, these attacks had an impact on the organization's capacity to safeguard its assets, generate revenue, win over clients' confidence, uphold its good name, and carry out its mission with efficiency and effectiveness. The petroleum industry and related systems, including the SCADA System, were vulnerable to cyberattacks, as seen in the accompanying picture, which also presents security countermeasures. Figure1 illustrates Cloud based SCADA Attacks and its security solutions.

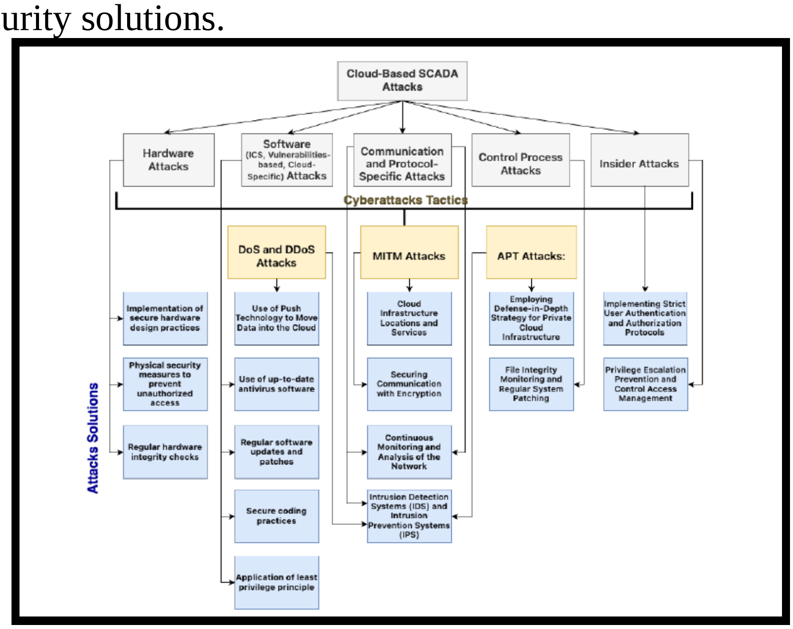
Cloud-Based SCADA Attacks
Hardware Attacks
Software (ICS, Vulnerabilities-based, Cloud-Specific) Attacks
Communication and Protocol-Specific Attacks
Control Process Attacks
Insider Attacks
Cyberattacks Tactics
DoS and DDoS Attacks
MITM Attacks
APT Attacks:
Attacks Solutions
Implementation of secure hardware design practices
Physical security measures to prevent unauthorized access
Regular hardware integrity checks
Use of Push Technology to Move Data into the Cloud
Use of up-to-date antivirus software
Regular software updates and patches
Secure coding practices
Application of least privilege principle
Cloud Infrastructure Locations and Services
Securing Communication with Encryption
Continuous Monitoring and Analysis of the Network
Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)
Employing Defense-in-Depth Strategy for Private Cloud Infrastructure
File Integrity Monitoring and Regular System Patching
Implementing Strict User Authentication and Authorization Protocols
Privilege Escalation Prevention and Control Access Management

Figure 1. Cloud based SCADA attacks and its security solutions. [1]

To protect organizations from security threats and maintain their assets, reputation and operations without interruption, many previous studies have addressed the creation of cybersecurity frameworks. This research paper will present the most important of these studies.

2. Literature Review

The first study presents a cybersecurity framework for organizations, addressing threats and risks. It provides controls, tools, and techniques for auditing, generating output reports and identifying cybersecurity gaps. Future work aims to implement integrated tools for comprehensive and time-saving auditing, aligning with recent technologies and security maturity levels[2].

The second study examines commonly used cybersecurity standards and frameworks, aiming to assist organizations in selecting the most suitable framework for their specific cybersecurity needs. It highlights the importance of implementing these standards to protect sensitive data and prevent cybercrimes. [3]

The third study aims to review exists IT and security governance frameworks, identifying their limitations such as complexity, high cost, high skill requirements, and time and resource requirements. A simple, dynamic, and adaptive cybersecurity governance framework is proposed to address these limitations. The framework includes nine components, five activities, four outcomes, and seven processes, making it easy to implement by any organization. The research also reviews widely used governance frameworks, proposes a simple, dynamic, and adaptive framework, and proposes key performance indicators to evaluate its effectiveness. [4]

The fourth study summarizes 50 empirical studies from 2014-2023 to identify factors influencing cybersecurity implementation in various countries. Four main themes were identified: individual, organizational, technological, and governmental roles. The authors proposed a comprehensive cybersecurity framework to help organizations proactively consider their strategy and implement appropriate security measures.[5]

The fifth study illustrates the importance of the ITIL and COBIT frameworks in improving IT governance in financial organizations are demonstrated by this study. Organizations may support their strategic objectives, improve operational efficiency, assure regulatory compliance, and strengthen their IT governance skills by using these frameworks successfully.[6]

The sixth study examines e-learning management systems because of lack of funding and understanding of cybersecurity issues. To safeguard (ELMS) in higher education institutions, a lightweight framework model is suggested. It has the benefit of providing customized protection, streamlined procedures, necessary controls, cybersecurity awareness training, and quick deployment, all of which enhance cybersecurity resilience in settings with limited resources. [7]

The seventh study explores the evolution of cyber resilience frameworks in network security, emphasizing their importance in operational continuity. Key components include risk assessment, threat intelligence, incident response, and recovery planning. Integrating resilience into business strategies allows informed decisions, resource allocation, and proactive risk management.[8]

The eighth study helps organizations prevent and mitigate data manipulation events by aligning their data integrity policy with the elements of the NIST Cybersecurity Framework. The paper reviews cybersecurity frameworks to identify the most a customizable option for organizations to address data manipulation risk, providing high-level guidance for mitigating cyber threats. Future work will focus on developing Profile for the NIST Cybersecurity Framework with data manipulation risk.[9]

After reviewing previous studies, it was found that they contributed to a limited extent in reducing the security threats facing organizations in general. Therefore, the need arose to develop a comprehensive framework for cybersecurity that reduces security risks. This proposed framework can be used to assist in strategic planning, reaching tactical demands that affect people, processes and technology, which directly affect organizations in general and the petroleum sector in particular.

3. The objective of the Framework

Organizations that adopt a cybersecurity framework accomplishes a number of objectives, such as creating a cohesive approach to managing IT risks internally, maturing IT controls internally, and effectively managing IT risks across organizations.

4. Framework Components

This research is Presented 22 domains, 5 functions, and 301 controls as part of the suggested framework. Table1 illustrates the proposed framework.

Table 1: The Proposed Framework

Domains	Number of controls related to functions				
	Identify	Detect	Protect	Recover	Respond
Asset Management	10	10	3	--------	--------
Secure Engineering & Architecture	--------	3	7	--------	--------
Physical security	1	4	9	--------	1
Endpoint Security	2	7	10	--------	3
Network Security	--------	6	10	--------	--------
Configuration Management	2	4	9	--------	--------
Change Management	--------	--------	10	--------	--------
Identification and Authentication	10	1	3	--------	--------
Cryptography	--------	--------	10	1	--------
Human Resource Security	1	1	8	--------	--------
Security Awareness & Training	3	------	9	--------	--------
Compliance	4	--------	5	--------	--------
Business Continuity & Disaster Recovery	--------	1	10	8	3
Security Operations	------	------	6	------	------
Threat Management	5	3	--------	--------	--------
Incident Response	2	4	3	1	10
Vulnerability & Patch Management	1	8	7	--------	--------
Third-Party Management	3	5	2	--------	1
Web Security	1	1	6	--------	--------
Cloud Security	9	1	6	--------	2
Maintenance	--------	3	7	--------	--------
Risk Management	10	1	3	--------	1

1. Asset Management

One of the roles in developing numerous cybersecurity standards that raises the profile of security specialists is managing all physical and virtual technological assets, from purchase to disposal to guarantee safe usage.[10]This domain contains three functions, and fifteen controls are, identify which contain ten controls, first control is Asset Governance refers to the process which an organization assigns accountability and decides on matters pertaining to projects, activities, actions, and concerns linked to asset management is known as asset management governance. Second is stakeholder identification & involvement, refers to the significance of involving stakeholders is increases stakeholders' knowledge of and commitment to the evaluation process, decreases their mistrust and anxiety of the review process, increases the likelihood of using the evaluation's findings strengthens the validity of the evaluation's conclusions. Third is asset inventories and categorization with component duplication avoidance which refers to conduct inventories of technology assets, include current systems, applications, and services in use, prevent duplication of assets. Fourth, is dynamic host configuration protocol (DHCP) server logging, refers to the server logging system records successful and unsuccessful lease grants, the server's IP pool being depleted, and message requests and their related acknowledgements. Fifth, is software licensing restrictions, refers to restricts software licensing to safeguard intellectual property (IP) rights; It works with three different kinds of software licenses. Restrictions: Copy left, proprietary, permissive. Sixth, is automated location tracking, refers to use customization as an organization-defined set of rules to track system components based on their geographic location. Seventh, is network diagrams and data flow diagrams (DFDs), which allude to Network flow diagrams are essential for mitigating risks, enforcing information security policies, and understanding the environments that include sensitive data, which shown on well-drawn network diagrams. Eighth, is secure disposal, destruction or re-use of equipment which prevents data leakage. Ninth, is brought your own device (BYOD) usage which set of rules in place at an organization that permits workers to access company data and applications using their own devices, laptops, tablets, phones, or anything else. Tenth, is system and database administrative processes, refer to the development, implementation, and management of database administration and system administration procedures, together with the associated standard operating procedures (SOP). Second function is Protect which contain three controls, first control is automated unauthorized component detection, refers to alert when unauthorized hardware and software components are detected. Second, is tamper detection and complies, refers with best practices, companies that need to guard against application tampering are also likely to need to avoid reverse engineering. Third, is Inspection of Systems, Components & Devices, refers with Systems and system components taken out of organization-controlled regions are subject to tamper resistance and detection inspections, which look for signs of both logical and physical manipulation. Third function is Detect which contain ten controls, first control is network access control (NAC), refers to enhance the security, and access management of a private network. It provides endpoint security protection through security policies and system authentication methods. Second, is removal of assets, refers to Systems that enter and leave organizational premises can be authorized, controlled, and tracked using established mechanisms. Third, is use of third-party devices, refers to safeguards in place to lessen the possibility that external assets connected to the network would damage company property or steal company information. Fourth, is tamper protection, refers to one component of anti-tampering capabilities is tamper protection, which also includes standard protective attack surface reduction guidelines. Fifth, is video teleconference (VTC) security and voice over internet protocol (VOIP) security which refer to prevent possible eavesdropping; it includes secure video conferencing (VTC) capabilities on endpoint devices and in specified meeting rooms, as well as secure IP telephony (IPT) that separates Voice over Internet Protocol (VoIP) data.

Sixth, is multi-function devices (MFD), refers to offer centralized document management in an office setting and integrates the capabilities of several devices into a single device. Seventh, is jump server, refers to be a computer system that serves as a network's gateway for connections with other devices. It was set up in a demilitarized zone (DMZ). Eighth, is database management system (DBMS), refers to implement and maintain Database Management Systems. Ninth, is radio frequency identification (RFID) security, refers to guarantees the use of RFID distribution to safeguard data integrity and confidentiality and stop unauthorized access to restricted areas. Tenth, is decommissioning, refers to a crucial procedure that enables the elimination of any business system or application from an organization's operations.

2. Secure Engineering & Architecture

Businesses match their decisions on cybersecurity engineering and architecture to their overall technology architectural strategy and industry. Cybersecurity architecture seeks to assist cybersecurity consultants in answering questions from executives such as: Are we secure? Are security investments delivering value to the business? What is our preparedness for a cyberattack? Offers a bird’s eye view of the organizations’ security posture; offer better control of the environment and an architecture that can be tailored to meet organizational needs and requirements.[11] This domain consists of Protect function and ten controls. First control is centralized management of cybersecurity and privacy controls, which centrally oversee the administration, execution of cybersecurity and privacy policies, as well as associated procedures, throughout the whole company. Second are defense-in-depth (DID) architecture, which involves layering a number of defensive techniques to safeguard sensitive data and information. Third are application partitioning, which is the division of user functionality, including user interface services, and information system management functions by the information system. Fourth are preventing program execution and memory protection, refers to there are automated systems in place to guard against unauthorized code execution and to stop unauthorized program execution from happening in system memory. Fifth are failed safe, which Follow the organization's established list of failure conditions and safety procedures while implementing fail-safe measures. Sixth are refreshing from trusted sources, which makes sure that data and software used for updates to information system components and services come from reputable and verified sources. Seventh controls are honeypots, which is a cybersecurity tool that draws hackers away from real targets by creating a fictitious attack target. They also obtain information about the identities, strategies, and objectives of enemies. Eighth controls are heterogeneity, which utilizing a range of information technologies for system components specific to a company. Ninth are virtualization techniques, which using virtualization technology to enable a company to install a range of operating systems and applications. Tenth are clock synchronization, which permits all important system clocks can be synchronized by mechanisms that make use of time-synchronization technology.

3. Physical Security

It refers to the measures and mechanisms implemented to safeguard physical assets, such as buildings, equipment, and personnel, from unauthorized access, theft, vandalism, or damage. It includes security measures such as access control systems, surveillance cameras, security guards, alarms, and locks. On the other hand, cybersecurity refers to the protection of digital assets, including data, networks, systems, devices, and applications, from cyber threats, such as hackers, malware, ransomware, and social engineering attacks.[12] There are four functions and fifteen controls in this domain, first function is Identify which consists of one control that is site security plan (site plan), refers to the procedures in place to record a Site Security Plan (Site Plan), which serves as a summary of the security measures put in place to safeguard technological assets from physical access, as well as relevant risks and threats. Second function is Detect which consists of four controls, first is searches, refers to prevent unauthorized exfiltration of data and technology assets, physical access control mechanisms are in place to inspect personnel and their personal effects. Second are intrusion alarms -surveillance equipment, refers to how organization monitors physical intrusion alarms and surveillance equipment. Third is fire detection devices, refers to use and maintain fire detection systems, devices that automatically activate and alert emergency responders in the event of a fire. Fourth is asset monitoring and tracking, refers to The process of using asset tracking hardware and software to remotely manage both movable and fixed assets, from laptops to shipping containers, and make sure valuable items remain safe and in good condition. Third function is Protect which consists of nine controls, first is role-based physical access, it is a function of network access control (NAC) that gives access and assigns permissions to users according to their roles in the company. Second is access to information systems, the organization keeps an eye on physical access to the information system. Third is distinguishing visitors from on-site personnel which makes it simple to tell onsite staff members from guests, particularly in locations where regulated or sensitive data is accessible. Fourth is supporting utilities refers to guard against damage and destruction to the system's power cabling and equipment. Fifth is emergency for all shutoff refers to the building which has safety features that allow power to be turned off in an emergency by put emergency stop switches or other devices close to systems to allow workers safe and convenient access. Sixth is redundant cabling refers to if one of the power lines are severed or otherwise damaged, electricity is guaranteed to continue flowing thanks to physically distinct and redundant cables. Seventh is fire suppression devices, refers to there are systems in place for facility security that make use of fire suppression equipment or systems that automatically alert emergency responders and organizational staff to any activation. Eighth is transmission medium security, refers to prevent data interception, interference, or damage to power and telecommunications cabling carrying data or supporting information services. Ninth is access control for output devices, refers to the organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output. Fourth function is Respond which consists of one control, is automatic fire suppression which offers an extra degree of fire protection.

4. Endpoint Security

It is a cybersecurity strategy which protects endpoints, like computers, laptops, and mobile devices, against hostile activities. A crucial part of preventing advanced persistent threats (APTs) at the endpoint level is the use of endpoint security solutions, such as antivirus software, host-based intrusion detection systems (HIDS), and endpoint detection and response (EDR) platforms.[13] There are four functions and twenty-two controls in this domain, first function is identify which contain two controls, first control is documented protection measures , refers to antimalware technologies are documented using this function. Second is notice of collection, refers to help people understand that organization-defined sensors are gathering personally identifiable information about them. Second function is detected which contain seven controls, first control is malicious code protection (anti-malware), refers to use malicious code protection methods, updates, configures them at information system entrance and exit points in order to find and remove malicious code. Second control is centralized management of antimalware technologies, refers to develop a centrally guard computers and information technology systems against harmful software. Third control is heuristic- non-signature-based detection, which makes use of heuristic and non-signature-based antimalware detection powers. Fourth control is evolving malware threats which identifies systems that are malware-free, this function periodically evaluates the hazards posed by emerging malware. Fifth control is always on protection, refers to safeguard that prevent non-privileged users from disabling or modifying them, unless they are granted explicit permission by management on an individual basis and for a restricted duration. Sixth control is integrity checks which verify setups by examining the software and firmware for integrity. Seventh control is mobile code refers to software programs or parts of programs obtained from remote systems, transmitted across a network, and executed on a local system without explicit installation or execution by the recipient. Third function is Protect which contain ten controls, first control is prohibited installation without privileged status, refers to software installations by users without specified privileged status are forbidden by the information system. Second control is software installation alerts, refers to when new software is found, an alert is generated. Third control is automatic antimalware signature updates which sets up all corporate assets to get automatic updates for anti-malware signature files. Fourth control is software firewall which uses to check data entering and leaving the device. The user can alter it to suit their requirements. Fifth control is endpoint file integrity monitoring (FIM), is a security procedure that keeps an eye out for evidence of potential cyberattacks by analyzing and monitoring the integrity of vital assets for signs of corruption or manipulation. Sixth control is hosting intrusion detection and prevention systems (HIDS/HIPS) refers to a program that keeps track of a single host's attributes and activities in order to spot and halt questionable conduct. Seventh control is automatic spam and phishing protection updates, which automatically update them in compliance with configuration and change management protocols. Eighth control is central management, refers to technologies for spam and anti-phishing is managed centrally by this department. Ninth control is port & input / output (I/O) device access, refers to disable or eliminate input/output devices or connection ports that are designated by the company. Tenth control is disabling - removal in secure work areas refers to collaborative computing devices which can be disabled or removed from secure work locations and vital information systems using existing mechanisms. Respond is the fourth function, is made up of three controls: integration of detection and response, which is the first control, entails tracking, monitoring, rectifying, and providing historical access to detected occurrence. Second control is automated notifications of integrity violations which use automatic systems that notify you when differences are found during integrity verification. Third control is automated response to integrity violations, refers to integrity breaches are found, the system should automatically shut down, restart, and implement.

5. Network Security

These domains aim to Create and put into practice defense-in-depth strategy that is both safe and robust and that upholds the principle of "least functionality" by limiting network access to systems, apps, and services. It can be manual and automatic configuration. It consists of two functions and thirteen controls. First function is Detect, which contains three controls. First is automated monitoring & control, which keeps an eye on and manage remote access sessions. Second is rogue wireless detection, refers to methods for detecting wireless access points (WAP) and classifying all Was in the building as approved or illegal. Third are route privileged network access, which permits to automated techniques to route networked, privileged accesses through a specific, controlled interface. Second functions are Protect, which contains ten controls. First is network segmentation, DMZ networks, refers to that Network segmentation may be achieved by mechanisms that divide information flows either physically or conceptually. Second are data loss prevention (DLP), DNS & content filtering, refers to methods to compel Internet-bound network traffic to pass via a proxy device like a Policy Enforcement Point (PEP) in order to filter the content of URLs and limit a user's ability to connect to unsafe or restricted websites. Additionally, data loss prevention (DLP) can be used to safeguard sensitive materials during handling, storage, and transportation. Third are remote session termination, session integrity, which ensures the confidentiality and authenticity of communications sessions, as well as to discontinue remote sessions at the conclusion of the session or during an inactivity period specified by the business. Fourth is protection of confidentiality- integrity using encryption, authentication and encryption, refers to protect by cryptographic protocols, which also insure wireless access through secure authentication and encryption. Fifth is network intrusion detection-prevention systems (NIDS/ NIPS), wireless intrusion detection/prevention systems (WIDS/WINS), refers to identify and prevent network intrusions. Sixth is zero trust architecture (ZTA), safeguarding data over open networks, which handles all users and devices as possible threats, preventing access to resources and data unless the users can be properly validated and given permission to access them. Seventh is end-user messaging technologies, electronic messaging, sender policy framework (SPF) refers to safeguard email communications' confidentiality, integrity, and availability; to prevent unprotected sensitive and structured data from being transmitted by end-user messaging technologies; authenticate email communications by configuring a DNS Sender Policy Framework (SPF) record to identify IP addresses and names. Eighth is work from anywhere (WFA), telecommuting security, which regulates remote workers' access to systems and data as well as to define safe telecommuting procedures. Ninth are third-party remote access governance, which proactively manage and keep an eye on third-party accounts that are used to remotely access, support, or repair system components. Tenth are intranets, route traffic to proxy servers, which process, stores, and transmits organization-controlled information using external systems, and to route internal communications traffic to external networks through organization-approved proxy servers at managed interfaces. Figure 2 illustrates automation for network security configuration.

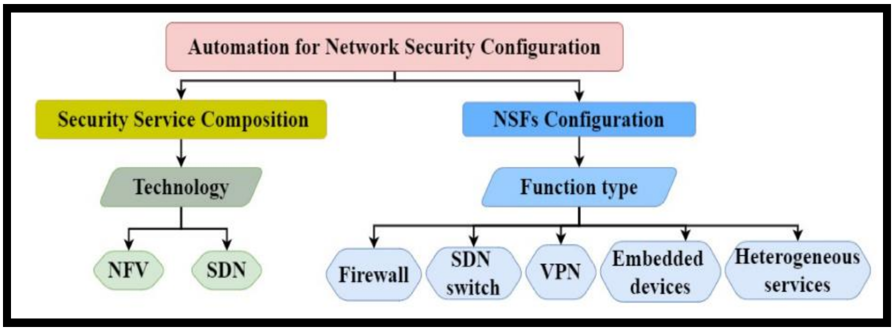

Figure2:Automation for Network Security Configuration[14]

6. Configuration Management

It considers one of the key components of network management, ensures that the setup and management of a network are done appropriately. The baseline is used to identify the software and hardware components that make up the specific versions of a system. In case of the failure of a new release, the baseline will be considered as a point to which to return. Some of the risks associated with the use of a VPN are poor configuration management.[15] There are three functions and Fifteenth controls considering the following, first function is Identify which contain two controls, first control is assignment of responsibility , refers to assign staff members inside the company who are not directly involved in system development the task of designing the configuration management procedure. Second is retention of previous configurations, refers to hardware, software; firmware, configuration files, configuration records, and related documentation are all being kept in their earlier iterations of the baseline configurations in order to facilitate rollbacks. Second function is Detect which contain Fourth controls, first is reviews & updates of responsibility, refers to which the company examines and modifies the information system's baseline setup. When necessary as a result of and as an essential component of updating and installing information system components. Second is automated central management & verification, refers to The availability, correctness, and consistency of configuration settings data can all be enhanced via automated tools (such as baseline configuration tools and hardening tools). Third is periodic review, refers to examine the system to find ports, protocols, applications, and services that are hazardous or superfluous. Fourth is unauthorized installation alerts, refers to unlawful software is found, these systems send out an alert so that staff members may handle the installation. Third function is Protect which contain Ninth controls. First is system hardening through baseline configurations, refer to apply the proper configurations, disabling unnecessary or underused services, and applying system patches, system hardening can be achieved. The rules that have been chosen and put into place to offer the strongest general level of system hardening are known as the baseline configuration. Second is development & test environment configurations, refer to reduce the possibility of unintentional modifications. There are mechanisms in place to maintain baseline configurations for development and test environments independently of operational baseline configurations. Third is network device configuration file synchronization, refers to set up to start and run configuration files. Fourth is the least functionality, refers to guarantee that information systems are set up to limit the usage of non-essential features like ports, protocols, and services, and to provide necessary capabilities. Fifth is prevented unauthorized software execution, refers to apply deny-by-exception (blacklisting) policy is the method this function utilizes to stop the use of unapproved software. Sixth is unauthorized or authorized software (blacklisting or whitelisting)**.** Blacklisting is the term used to describe the procedure used to identify software programs that are not allowed to execute on systems. Whitelisting is the term used to describe the procedure used to determine which software applications are allowed to run on systems. Seventh is unsupported internet browsers & email clients, refers to permit the use of authorized email clients and web browsers on computers. Eighth is a user-installed software, refers to be necessary for the operating system to stop non-privileged users from carrying out privileged operations. Ninth is sensitive-regulated data actions, refers to information that has to be encrypted to avoid unauthorized access or interception, whether it is during transmission or storage, as it might cause unintentional harm to the person to whom it belongs. Configuration management is an operational metrics which overall count of upgraded and patched systems.

7. Change Management

The collection of procedures known as change management makes sure that every modification made in an IT environment is regulated and carried out reliably. Ensuring that any proposed changes to an IT environment are suitably risk-averse and that they will not conflict with one another or with other scheduled or unexpected operations are the primary goal of change management. IT systems will be configured inconsistently without efficient change and configuration management, which frequently results in exploitable vulnerabilities that might cause security incidents. To makes changes to the system that will either temporarily or permanently solve it, employ the change management and configuration management procedures.[16] It consists of three functions and eight controls. First function is Identify, which has one control called report verification results, a few examples of organizational staff who would be interested in the security function verification results are information security managers, senior information security officers, and information systems security officers. Second function is Detect, which has one control called automated access enforcement- auditing, which reviews configuration change logs after the fact to find any illegal modifications. Third function is Protect, which contains six controls, first is signed components, refers to safeguards which stops software and firmware components from being installed unless it has been confirmed that the component has been digitally signed with a certificate that the organization has accepted and approved. Second controls are dual authorization for change, which makes sure that no modifications can be made to certain information system components or data unless they are carried out by two authorized personnel. Third functions are limit production-operational privileges, which restricts the operational powers needed to make changes. Fourth controls are library privileges, refers to limit access to software libraries to those who have a legitimate business need for them. Fifth controls are stakeholder notification of changes, which makes that interested parties are informed about and comprehend the implications of proposed changes. Sixth controls are security functionality verification, which abnormalities are detected, there are procedures in place to confirm that security controls are operating as intended.

8. Identification and Authentication

It aims to apply the principle of "least privilege" by granting authorized individuals exclusive access to the organization's data and systems.[17] This domain consists of three functions and twelve controls. First function is Identify, which consists of one control that is attribute-based access control (ABAC), refers to keep things like information, network hardware, and IT resources safe from unwanted access and usage. Second function is Protect which consists of ten controls, first is acceptance of pin credentials, refers to acknowledge and electronically confirm credentials that comply with Personal Identity Verification. Second control is identification & authentication for devices related with third party systems services, which refers to recognize and validate the systems and services of third parties. Third control is the least privilege and network access to non-privileged accounts, refers to take use of both the multifactor authentication (MFA) and the least privilege concepts when granting unprivileged accounts access to the network. Fourth control is multifactor authentication (MFA) and local access to privileged accounts, refers to methods for authenticating privileged accounts' local access using Multi-Factor Authentication (MFA). Fifth control is role-based access control (RBAC), refers to restrict network access according to an individual's function within an organization is known as role-based access control, or RBAC. Sixth control is password managers and automated support for password strength, refers to protect and store passwords via a password manager, and to determine whether password authenticators are strong enough to meet their length and complexity requirements. Seventh control is hardware token-based authentication and biometric authentication, refers to an organization-specified biometric quality criteria for false positives and negatives. As well as organization-specified hardware token quality requirements for authentication, are satisfied via mechanisms ensuring biometrics-based authentication. Eighth control is account lockout, removal of temporary/emergency accounts, refers to automatic mechanisms disable or delete temporary and emergency accounts. It set a limit on the number of unsuccessful login attempts made by the user in a row, and lock the account automatically when the organization-specified maximum number of unsuccessful attempts is reached after a certain amount of time for each kind of account. Ninth control is single sign-on (SSO), refers to a session and user authentication service that allows a single set of login credentials - such as username and password - to be used to access multiple applications. Tenth control is Session lock and termination, refers to a session ends, or a user requests it after a predetermined amount of inactivity, the organization has automatic procedures in place to log people out, either locally on the network or remotely. Third function is Respond which contain one control that is emergency accounts, refers to organization-specified time period for each sort of account, the information system automatically deletes, disables temporary, and emergency accounts.

9. Cryptography

It is the process of hiding or coding information so that only the person a message was intended for can read it. The art of using cryptography to secure data is called encryption. Cryptography serves the purposes of data security maintenance and safeguarding the integrity, confidentiality, and authenticity of the information via various kinds of crypto algorithms.[18] It consists of two functions and eleven controls, first function is Protect which consists of ten controls, first is use of cryptographic controls, refers to a vital line of defense against several dangers, such as illegal access, data breaches, manipulation, and eavesdropping, is cryptographic controls. Second control is alternate physical protection, refers to use cryptographic techniques to identify changes to data while it is being sent and prevent unauthorized exposure of information, unless alternative physical protections specified by the organization provide protection. Third control is transmission confidentiality and integrity which Preserves the integrity and confidentiality of any sent data. Fourth control is storage media, refers to safeguard the integrity and confidentiality of sensitive or regulated data stored on storage media, cryptographic procedures are in place. Fifth control is offline storage, refers to any storage device that has to be physically inserted into a system each time a user wishes to view or change data is referred to as offline storage. Sixth control is database encryption, refers to safeguard in place to guarantee that database servers encrypt data in order to preserve its secrecy. Seventh controls are wireless access authentication & encryption, which refers to encryption, user and device authentication help safeguard wireless access to the system. Eighth control is cryptographic key management, refers to controls are made possible by mechanisms that safeguard the confidentiality, availability, and integrity of keys. Ninth control is control & distribution of cryptographic keys, which refers to methods for distributing symmetric and asymmetric cryptographic keys securely that make use of key management procedures and technology that are widely accepted in the industry. Tenth controls are transmission of security & privacy attributes, refers to connect the information shared across systems and between system components with security and privacy features set by the company. Second function is Recovery which has one control that is availability, refers to Ensure that data is still accessible in the event that users misplace their cryptographic keys.

10. Human Resource Security

These domains aim to develop a workforce that is sensitive to privacy and cybersecurity by implementing ethical hiring procedures and continuing personnel management. Organizations' entire security posture can be improved by adopting human-centered approach to a cybersecurity design and decision-making. Businesses may better address the behavioral and cognitive aspects of security by integrating human factors considerations into cybersecurity procedures, which will ultimately increase their resilience against cyber threats. Comprehending the correlation between human factors and cybersecurity practices yields valuable insights that guide the development of intervention and training programs, to reduce dangerous cybersecurity practices.[19] It consists of four functions and eighteen controls. First function is identifying which contains nine controls. First controls are users with elevated privileges, refers to guarantee that any user, who gains access to a system that handles, retains, or transfers sensitive data has undergone clearance and ongoing training on how to manage it. Second controls are roles & responsibilities, refers to specify each employee's role in cybersecurity. Third controls are user awareness, which is an essential part of a company's overall security plan. It entails teaching staff members about the several cyber threats they can run across on a daily basis as well as how to reduce the risks. Fourth controls are competency requirements for security-related positions, which guarantees that people with the requisite qualifications fill all security-related roles. Fifth controls are roles with special protection measures, which makes sure that everyone using an information system to handle, store, or send data that needs extra protection possess legitimate access authorizations as evidenced by their official government duties. Sixth controls are rules of behavior, refers to establish, distribute the rules outlining the obligations, appropriate conduct for information, system usage, security, and privacy to those who need access to the system. Seventh controls are social media & social networking restriction, which uses of social media, networking sites, publishing content on for-profit websites, and disclosing account information are all expressly prohibited under rules of behavior. Eighth controls are use of mobile devices, which controls the business risks related to allowing mobile devices to access corporate resources. Ninth controls are third-party personnel security, which outlines the conditions for personnel security, such as security roles and duties, ensures that personnel security rules and procedures are followed. Second function is Detect, which contains one control that is probationary periods, refers to be a trial period of employment, subject to the employee's successful completion of the probationary requirements. Third function is Protect, which contain six controls. First is asset collection, refers to recover assets owned by the organization when worker's employment is terminated. Second controls are automated employment status notifications, which disable access to system resources and inform staff of specific termination actions using organization-defined procedures. Third controls are separation of duties (SOD), which are Alludes to the idea that no user should be granted sufficient rights to abuse the system on their own. Fourth controls are two-person rule, when making modifications to crucial assets, there are procedures in place to enforce the two-person rule. Fifth controls are identifying critical skills & gaps refers to assess the essential cybersecurity and data privacy competencies required to uphold the organization's objective and pinpoint any deficiencies. Sixth controls are performing succession planning, which mitigates the loss of highly skilled security personnel and the risks linked to extended job openings. Fourth functions are Respond, who contains two controls. First are personnel sanctions, which provide formal penalties approach for those who violate established privacy, information security rules, and procedures. Second controls are workplace investigations, refers to when there is a good chance that a policy has been broken, there are procedures in place to look into employee wrongdoing.

11. Security Awareness & Training

The goal of this domain is to cultivate a workforce that is concerned about cybersecurity and privacy by providing continuous user education regarding new risks, compliance requirements, and safe workplace practices. Tailored training programs are essential for firms to mitigate possible breaches by equipping workers to identify and address cyber threats. To create and implement good cyber hygiene practices both inside enterprises and among individual users, cybersecurity awareness is essential. Three primary categories can be used to group the fundamental ideas of cybersecurity awareness: knowledge, attitudes, and behaviors. Since conduct has a direct impact on people's and organizations' security postures, changing behavior is frequently the ultimate goal of cybersecurity awareness campaigns.[2] It consists of two functions and twelve controls, first function is Identify which consists of three controls , first is cyber threat environment, refers to there are systems in place to offer role-based training aimed at increasing user understanding of data privacy and cyber dangers. Second control is continuing professional education (CPE) cybersecurity and privacy personnel, which refers to stay competent and fulfill their designated tasks and responsibilities, mechanisms are in place to guarantee that they get continuing professional education(CPE)training. Third control is continuing professional education (CPE)- DevOps personnel, refers to guarantee that employees working in application development and operations (DevOps) have Continuous Professional Education (CPE) instruction in Secure Software Development Practices (SSDP), so they can effectively handle emerging risks. The second function is Protect which consists of nine controls, first control is security & privacy awareness, refers to guarantee that all workers and contractors receive the proper awareness training and education related to their job function. Second is simulated cyberattack scenario training, refers to a procedure intended to evaluate, in a secure and controlled setting, an organization's security posture against both known and developing threats. Third is social engineering & mining, refers to educate people in literacy about identifying, reporting real, possible cases of social engineering and social mining. Fourth is role-based security & privacy training, which refers to an organization choose the training's curriculum depending on the tasks and duties that are allocated to each employee as well as the systems' and organizations' security and privacy needs. Fifth is practical exercises, which Provides hands-on security and privacy training exercises that support the learning goals. Sixth is suspicious communications & anomalous system behavior, refers to offer staffs that have received the necessary training as part of a comprehensive security plan to ward against harmful code that infiltrates businesses through email or online applications. Seventh is vendor security & privacy training, refers to incorporate vendor-specific security training in support of new technology initiatives. Eight is privileged users, which provides training for privileged users to ensure these users understand their unique roles and responsibilities. Ninth is security & privacy training records, refers to record, store, and keep track of individual training activities.

12. Compliance

Companies make sure controls are in place to guarantee compliance with internal corporate standards and relevant legal, regulatory, and contractual compliance requirements. Cybersecurity awareness plays an important role in shaping attitudes and intentions towards information security policy compliance.[20] First function is identify, refers to statutory, regulatory & contractual compliance information security obligations included in contracts, laws, regulations. Other legal frameworks are intended to guarantee that businesses are taking the necessary precautions to safeguard confidential data and guard against abuse or unauthorized access. Second control is compliance scope, refers to inspect all of your devices and the people who are permitted to access protected data when thinking about compliance inside your operations. You should also make sure that the third parties you work with are abiding by compliance regulations. Third control is audit activities, refers to reduce the impact of audit-related activities on company operations, procedures are in place for carefully planning audits with input from operational risk and compliance partners. Second function is detecting, which is consists of five controls, first is cybersecurity & data privacy controls oversight, refers to offer an executive leadership-level supervision role for cybersecurity and data protection regulations. Second control is internal audit function, refers to put in place an internal audit function that can give top management insight into whether the organization's information governance and technology policies are adequate. Third control is security & data protection assessments, refers to make sure managers follow the proper cybersecurity and data protection policies, standards, and other applicable regulations by routinely reviewing the processes and written procedures under their purview. Fourth controls are independent assessors, refers to use assessment teams or independent assessors to do out control evaluations. Fifth controls are functional review of security and data protection controls, refers to periodically check that the organization's cybersecurity and data protection rules and standards are being followed by IT assets. Third function is Protect which consist of two controls, first is investigation access restrictions, refers to that an official investigation are supported by mechanisms that grant government investigators " the least privileges" and "least functionality" to guarantee that government. Second controls are government surveillance, refers to safeguards that prevent the host government from having unfettered and unmonitored access to the organization's services, applications, and systems, which might be a violation of all the organization's commitments. Fourth function is Respond, which consists of one control that is non-compliance oversight, refers to record and examine cases of non-compliance with all obligations in order to create suitable risk mitigation plans.

13. Business Continuity & Disaster Recovery

The four plans are referred to as information system contingency plan (ISCP), disaster recovery plan (DRP), critical information infrastructure protection plan (CIIPP)), and business continuity plan (BCP) in general. Business continuity is the ability of an organization to carry on providing goods and services at a reasonable level following an interruption. Whereas reactive and corrective measures are what trigger catastrophe recovery strategy. The purpose of a disaster recovery plan (DRP) is to resume business operations (processes and services) in a new location only in cases where relocation to a different location is required.[21] This domain consists of four functions and twenty-two controls, first function is Respond which contains three controls, first control is electronic discovery (E-Discovery), refers to the electronic process of locating, gathering, and delivering electronically stored information (ESI) in response to a production request in a legal action or inquiry. Second is restoring within time period, refers to recover system components from information that is integrity-protected and configuration-controlled is provided by this function. Third is AI & autonomous technologies incidents refers to procedure in place to deal with malfunctions or events involving high-risk autonomous technologies (AAT) and artificial intelligence (AI). Second function is Detect which contain one control, refers to contingency plan root cause analysis (RCA) & lesson learned, refers to that root cause analysis is a methodical and consistent way for organizations to utilize the lessons they've learned from past triumphs and mistakes to enhance performance in the future. Third function is Protect which consist of ten controls, first is established and move to an alternative storage location, refers to establish an alternate storage site to permit the storage and recovery of system backup information. Second is separate storage for critical information, refers to The backup copies are kept by the organization in a different location or a fire-rated container that isn't near the active system. Third is separation of primary-alternate providers, refers to Obtain alternate telecommunications services from providers other than the principal service providers is one way this function helps to lessen exposure to various hazards, such as the dangers of cyberattacks and natural catastrophes. Fourth is data backups and cryptographic protection, refers to safeguard data in the event of a disaster, accident, or malicious act, it is common practice to copy data from a primary location to a secondary location. This process involves the use of encryption to preserve the confidentiality and integrity of data stored on digital media during transfer outside authorized areas. Fifth is tested restoration using sampling, refers to test for contingency plans, it restores some system functionalities using a sample of backup data. Sixth is redundant secondary system, refers to Maintain a redundant secondary system that is separate from the primary system and that may be triggered without causing data loss or interruption to operations in order to do system backups. Seventh is dual authorization “two-person control” for backup media destruction, refers to make guarantee that backup data cannot be erased or destroyed unless two authorized people complete the job. Eighth is backup access, refers to limit privileged users with designated responsibilities for data backup and recovery activities to accessing backups. Ninth is information system recovery & reconstitution, refers to guarantee that, in the event of a disruption, compromise, or failure, systems may be safely recovered from and reconstructed to a known state. Tenth is backup & restoration hardware protection, refers to necessary technical and physical protection of the firmware, software, and backup and restoration hardware is ensured by established procedures. Fourth function is Recovery which consist of eight controls, first is resumed all missions & business functions, refers to the contingency plan activates. There are procedures in place to allow all missions and business operations to restart within Recovery Time Objectives (RTOs). Second is recovery time point objectives (RTO/RPO), refers to determine, evaluate, and justify workable methods for the business continuity plan which is provided by the RPO/RTO in conjunction with a business impact study. Third are automated training environments, refers to offer a more comprehensive and realistic incident response training environment, the company uses automated methods. Fourth is contingency planning and updates, refers to ensure that backup plans are up-to-date with changes in technology, business requirements, and input from testing activities. Fifth is the reliability and integrity test, refers to ensuring the integrity of the information, the reliability of the media, and that the company tests backup data. Sixth is failover capability, refers to the capacity for effortlessly and instantly transition to a dependable backup system. Seventh is isolated recovery environment, refers to use both a dedicated network infrastructure separates from the production environment and tools such as retention locking, role-based access control (RBAC). Eighth is reserve hardware, refers to a procedure in place to buy and keep an adequate stock of replacement hardware so that, in the case of a supply chain interruption, vital missions and commercial operations can continue.

14. Security Operations

Carry out data privacy and cybersecurity operations to produce high-quality services and safe systems, apps, and services that satisfy the commercial requirements of the company. It consists of one function and six controls, first function is Protect and first control is operations security, refers to throughout the system development life cycle, use organization-defined process security measures to safeguard critical organizational information. Second is standardized operating procedures (SOP), refers to a procedure which is a documented collection of guidelines that outlines the precise steps that need to be followed in order to carry out a regular task. It offers the standards, procedures, and guidelines required for the company to be successful. Third is security concept of operations (CONOPS) which creates a security Concept of Operations (CONOPS) for the information system that, at the very least, outlines how the company plans to run the system from an information security standpoint. Fourth is service delivery (business process support), refers to a company or service provider gives consumers access to IT services, such as apps, data storage, and other corporate resources, it is known as service delivery. Fifth is security operations center (SOC), refers to a centralized function that uses people, procedures, and technology to prevent, identify, analyze, and respond to cybersecurity incidents while also continually monitoring and strengthening the organization's security posture. Sixth is secure practices guidelines, refers to help with the setup, installation, and usage of the product and service, mechanisms that offer advice and guidance for their secure use are in place. Figure 3 illustrates the operation model for SOC.

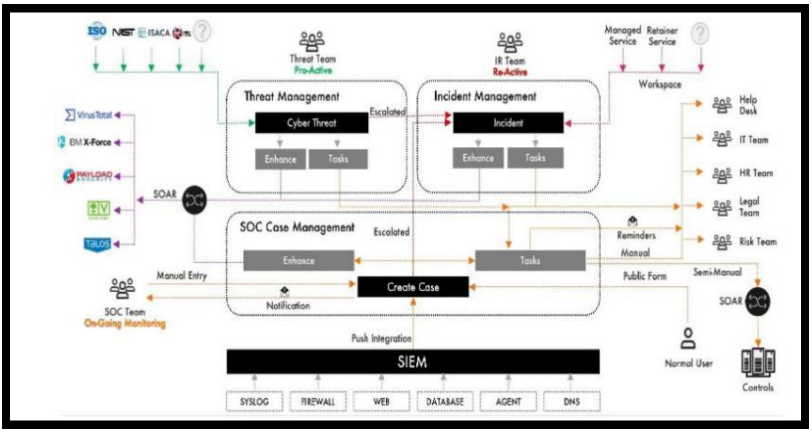

Figure 3 : The operation model for SOC. [22]

15. Threat Management

Cyber threat intelligence (CTI) is being used by enterprises more and more as a proactive way to strengthen their cybersecurity posture. By employing threat intelligence and promoting collaboration within the cybersecurity sector, organizations can strengthen their defenses and better protect their critical assets and data from assaults. By using preemptive measures and analyzing security-related data, organizations may foresee emerging threats, weaknesses, and attack trends, thereby managing cyber dangers. For example, businesses can use threat intelligence to identify any weaknesses in their security posture, prioritize security investments, and put in place additional controls or safeguards in order to secure critical assets and data. Moreover, security awareness training programs that utilize threat intelligence can help employees recognize and efficiently defend against common cyberattacks.[23] This domain consists of two functions and eight controls. First function is Identify which consists of five controls. First is threat intelligence program, which enhances the efficacy of exchanging threat intelligence data, utilize automated processes. Second is indicators of exposure (IOE), refers to create Indicators of Exposure (IOE) that help identify possible avenues of attack that an attacker could choose to target the company. Third is threat intelligence feeds, refers to that security teams can discover risks with the use of external data streams called threat intelligence feeds. Fourth is insider threat program, refers to identify, track down, and lessen the impact of insider activity that might endanger national security. Fifth is insider threat awareness, refers to use security awareness training to identify and report any insider threat indicators. Second function is Detect which consists of three controls, first is vulnerability disclosure program (VDP), refers to the fact that anybody may use a centralized process known as a VDP to report security flaws in an organization's internet-facing application. Second is threat hunting, refers to the process of aggressively investigating a network for hidden cyber threats. Third is tainting, refers to the act of incorporating hidden features into data, systems, or system parts so that organizations may be informed when information is being exfiltrated.

16. Incident Response

Create and maintain an incident response strategy that outlines what to do in the event of a malware event. This includes recovery techniques, containment strategies, and communication protocols. Benefits include: reduced downtime and data loss so that the incident response team is engaged, allowing for a coordinated and effective response to security issues.[24] This domain contains five functions and twenty controls, first function is Recovery which consists of one control is public relations & reputation repair, refers to oversee the incident's public relations and takes action to restore the organization's image. Second function is Detect consist of four controls. First is situational awareness for incidents, refers to document, monitor, report the status of cybersecurity and privacy incidents to internal stakeholders through incident resolution. Second is automated tracking, data collection and analysis, refers to how the company uses automated systems to help with incident information gathering and analysis, as well as security event tracking. Third is automated reporting, refers to streamline the various stages of report creation and analysis by utilizing analytics, business intelligence, and automation tools. Fourth is cyber incident reporting for sensitive data, refers to how promptly report events involving sensitive or regulated data. Third function is Protect consist of three controls, first is incident response operations, refers to The process by which an organization responds to a cyberattack or data breach in order to lower the likelihood of similar occurrences in the future. Second, is insider threat response capability, refers to procedure in place to manage an insider threat program. Third, is coordination with related plans, refers to determine whether an insider will use their authorized access to harm a company's information or equipment on purpose or accidentally. Fourth function is Respond consist of ten controls, first is automated incident handling processes, refers to how the organization employs automated mechanisms to support the incident handling process. Second is dynamic reconfiguration, refers to that Dynamic reconfiguration is part of the organization's incident response capability. Third, is Indicators of Compromise (IOC), refers to it is a digital forensic tool that indicates the possibility of an endpoint or network being breached. Fourth, is incident response plan (IRP) with its practices, refers to that an organization's response to cybersecurity incidents can be guided by an incident response plan that is structured and documented. Fifth is incident response testing, refers to measure the effectiveness and identify potential weaknesses or deficiencies, organizations test their incident response capabilities, while also providing more comprehensive and realistic incident response training environments. Sixth, is integrated security incident response team (ISIRT), refers to investigate of computer security incidents and proactive threat assessment, mitigation planning, incident trend analysis, security architecture review, and vulnerability management. Seventh, is incident stakeholder reporting, refers to how promptly reporting issues to relevant internal stakeholders, impacted clients and third parties, and regulatory bodies. Eighth, is vulnerabilities related to incidents, refers to how reported incidents that reveal system vulnerabilities are analyzed by specialists such as regulatory staff and the risk executive. Ninth, is root cause analysis (RCA) & lessons learned, refers to that root because analysis is an essential tool for learning lessons from successes and failures, and applying them to improve future performance. Tenth, are detonation chambers (sandboxes), refers to as dynamic execution environments, provide a secure environment in which untrusted or suspicious applications can run URL requests to check if they contain malicious code. Fifth function is identifying which consist of two controls, first is continuous incident response improvements, refers to Organizations utilize metrics and assessment criteria to assess incident response programs to help with incident response operations. Second is regulatory & law enforcement contacts, refers to How to keep in touch with relevant law enforcement and regulatory bodies about incident response.

17. Vulnerability & Patch Management

Patch management is an unwavering line of defense against online threats. Operating systems and software have known flaws that can be exploited. Patching and updating security updates on a regular basis is similar to fixing weak points. The quick identification of new vulnerabilities makes timely patch management a crucial procedure. It makes sure that possible points of entry are blocked off before adversaries may take advantage of them. Automated patch management systems expedite the procedure, enabling establishments to promptly address emergent risks. Organizations may prevent exploitation and show stakeholders and consumers that they are committed to cyber security by keeping their systems up to date.[25] This domain consists of three function and sixteen controls. First function is Identify which consists of one control that is trend analysis, refers to automate methods for comparing vulnerability scan findings over time to identify patterns in system vulnerabilities. Second function is Detect which consists of eight controls, first is review historical event logs, refers to examine past audit records to see if the discovered vulnerability has ever been used within a time frame particular to the company. Second control is external vulnerability assessment scans, refers to scan for external vulnerabilities or perimeters is done from a location other than the present network. Third control is correlate scanning information, refers to identify the existence of multi-vulnerability/multi-hop attack vectors, the organization compares the results of vulnerability scanning tools. Fourth is penetration testing, refers to a cyber-security specialist looks for and attempts to take advantage of weaknesses in a computer system. Fifth is independent penetration agent or team, refers to conduct penetration testing on the information system or system components, the company hires a separate penetration agent or penetration team. Sixth is technical surveillance countermeasures security, refers to a technique that finds and disables electronic eavesdropping instruments such as microphones and concealed cameras. Seventh is reviewing vulnerability scanner usage, which makes sure that scanning activities are restricted to the times of valid scans. Eighth control is red team exercises, refers to an exercise that simulates an adversary attempt to compromise corporate missions and business operations in real-world settings in order to offer a thorough evaluation of the information system and organization's security capabilities. Third function is Protect which consists of seven controls. First is attack surface scope, refers to that an attacker's point of entry, point of impact, point of data extraction from a system, system element, or environment is the collection of points on its border. Second is continuous vulnerability remediation activities, which describes the procedure for locating and resolving security flaws or vulnerabilities in networks, systems, or software. Third is automated software & firmware patching and updates which install security-related firmware and software upgrades on system components that are specific to the company automatically. Fourth is automated remediation status, refers to check to see whether any system components have the necessary security-relevant software and firmware upgrades installed through automated processes established by the organization. Sixth is time to remediate-benchmarks for corrective action, refers to calculate the average time needed to fix system flaws, organizations establish guidelines on when to take corrective action. Seventh is removal of previous versions, refers to follow the installation of upgraded versions. Eighth is update tool capability, refers to use technologies for vulnerability scanning that allow it to easily update the information system vulnerabilities that need to be examined.

18. Third-Party Management

Businesses make sure that the risks to cybersecurity and data privacy posed by third parties are kept to a minimum and have contingency plans in case a third party is hacked, loses its credibility, or goes out of business. Third-party risk management is not merely a compliance requirement; it is a strategic imperative for superannuation organizations committed to safeguarding member interests and ensuring long-term stability.[26] It consists of three functions and fifteen controls. First function is Identify which contain ten controls. First are third-party inventories and services, refers to how systems mitigate risks related to third parties and to keep an up-to-date, accurate, and comprehensive list of external service providers. It may have an impact on the confidentiality, integrity, availability, and integrity of an organization's systems, applications, services, and data. Second is third-party risk assessments, refers to an examination of the dangers that third-party interactions along the supply chain bring to your company. Third is third-party contract requirements, refers to a procedure in place to impose contractual obligations on cybersecurity and data privacy with third parties. It reflects the necessity for the organization to safeguard its data, systems, and procedures. Fourth is third-party scope review refers to the responsibility, accountability, supportive, advisory, and informed (RASCI) matrix which have mechanisms in place to be regularly verified to guarantee that cybersecurity and data privacy control functions appropriately represent stakeholder duties and compliance. Fifth is third-party incident response & recovery capabilities, refers to guarantee that testing and reaction recovery plans are carried out with essential suppliers. Sixth control is review of third-party services, refers to give project stakeholders confidence and maybe serving as a need for insurance, a Third-Party Review or due diligence procedure can provide legitimacy to new or developing technology. Seventh control is limiting potential harm, refers to prevent harm from prospective adversaries identifying and attacking the organizational supply chain, the company uses well-defined security measures. Eight controls are processes to address weaknesses or deficiencies, refers to sets up a procedure to fix any flaws or shortcomings in supply chain components found by organizational or independent evaluations of such components. Ninth controls are external connectivity requirements-identification of ports, protocols & services, refers to procedures in place that mandate external service providers (ESP's) to determine and record the ports, protocols, and other services that the organization needs in order to run its technologies and operations. Tenth control is responsible, accountable, supportive, consulted & informed (RASCI) matrix, refers to track and record the allocation of cybersecurity and data privacy controls between external service providers and internal stakeholders. Second function is Detect, which consists of one control that is security compromise notification agreements, refers to require external service providers (ESP's) to notify the organization of any real or suspected supply chain breaches that might negatively impact its systems, applications, and services. Third function is Protect, which consists of four controls, first is contract flow-down requirements, refers to guarantee that contracts that apply to suppliers and subcontractors that fall within the purview of cybersecurity and data privacy are covered. Second control is third-party authentication practices, refers to guarantee that external service providers (ESP's) employ distinct authentication factors for every client. Third control is breaking clauses, refers to put "break clauses" in contracts that allow for noncompliance with cybersecurity and data privacy requirements.

19. Web Security

This area protects networks, servers, and computer systems from theft or damage to hardware, software, or data. Part of it involves safeguarding computer systems against being misdirected or interfering with the services they are meant to provide. It consists of three functions and eleven controls. First function is Identify, which has one control that is cookie management, refers to give people accurate and lucid information about cookies in compliance with legal obligations regarding cookie management. Second function is Detect which has one control that is website change detection, refers to when illegal additions, deletions, modifications occur on websites that handle, store, transport sensitive or regulated data, there are mechanisms in place to identify and address these Indicators of Compromise (IOC). Third function is Protect, which contains eight controls. First is unauthorized code, refers to make sure that a secure page doesn't include any illegal code when it is shown in a client's browser. Second controls are use of demilitarized zones (DMZ), refers to that a local area network (LAN) is frequently isolated from other untrusted networks, such as the public internet, by a physical or logical subnet called a DMZ. Third controls are web application firewall (WAF), which contributes to web application security. Generally, it defends online applications against several types of attacks, including file inclusion, SQL injection, cross-site scripting (XSS), and cross-site injection. Fourth controls are web security standard, refers to that secure systems' development lifecycle (SSDLC) processes within the company are designed to incorporate the open web application security project (OWASP) Application Security Verification Standard. Fifth controls are web application framework, refers to facilitate the creation of web applications, including web services, web resources, and web APIs. Sixth controls are validation & sanitization which determines if an input satisfies a set of requirements. Sanitization alters the input in order to guarantee that it is. Seventh controls are output encoding, refers to be an essential safeguard against XSS assaults. It can help you protect user data and preserve the integrity of your online application by stopping dangerous scripts from being run by users' browsers. Eighth controls are secure web traffic and web browser security, which employs the content-security-policy, HSTS, and X-Frame-Options response headers to safeguard users and the web application itself.

Figure 4 illustrates the Web Security tools as a technical solution for cyber security solution.

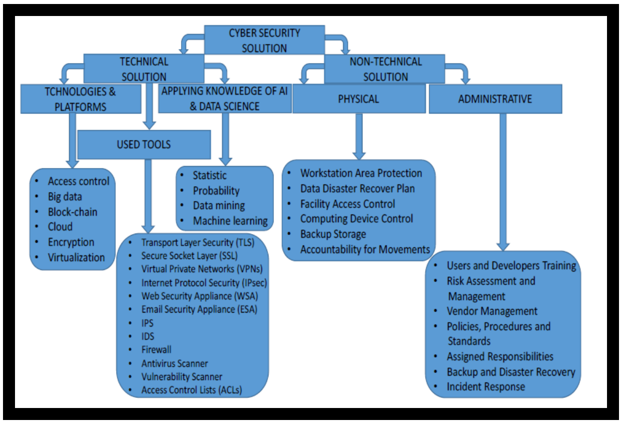
CYBER SECURITY SOLUTION
TECHNICAL SOLUTION
NON-TECHNICAL SOLUTION
TCHNOLOGIES & PLATFORMS
APPLYING KNOWLEDGE OF AI & DATA SCIENCE
PHYSICAL
ADMINISTRATIVE
USED TOOLS
Access control
Big data
Block-chain
Cloud
Encryption
Virtualization
Statistic
Probability
Data mining
Machine learning
Transport Layer Security (TLS)
Secure Socket Layer (SSL)
Virtual Private Networks (VPNs)
Internet Protocol Security (IPsec)
Web Security Appliance (WSA)
Email Security Appliance (ESA)
IPS
IDS
Firewall
Antivirus Scanner
Vulnerability Scanner
Access Control Lists (ACLs)
Workstation Area Protection
Data Disaster Recover Plan
Facility Access Control
Computing Device Control
Backup Storage
Accountability for Movements
Users and Developers Training
Risk Assessment and Management
Vendor Management
Policies, Procedures and Standards
Assigned Responsibilities
Backup and Disaster Recovery
Incident Response

Figure 4 : Web Security tools as a technical solution for cyber security solution [27]

20. Cloud Security

This domain aims to manage cloud instances as an addition to on premise technology with security safeguards that are at least as strong as those found in the company's internal cybersecurity and data privacy policies. The figure below illustrates a cloud computing as a cybersecurity solution. It consists of two functions and nine controls. First function is Identify which consists of four controls, first is customer responsibility matrix (CRM), refers to formal mechanisms for recording a customer responsibility matrix (CRM) that outlines the allocated control duties between the cloud service provider (CSP) and its clients. Second is multi-tenant event logging capabilities, refers to that managed security service providers (MSSPs) and multi-divisional businesses may offer security services to several client organizations with a single deployment thanks to multitenant environments. Second are multi-tenant forensics capabilities, refers to guarantee that multi-tenant service providers (MTSP) enable quick forensic investigations in the case of a verified or suspected security incident. Third are multi-tenant incident response capabilities, refers to guarantee that multi-tenant service providers (MTSP) enable quick reaction to security events and vulnerabilities that are verified or suspected, along with timely communication of impacted clients. Second functions are Protect which consists of four controls, first is data handling & portability, refers to guarantee that cloud providers handle data in cloud-based services securely, including during import, export, and management. Second are geolocation requirements for processing, storage, and service locations, refers to manage the location of cloud processing and storage in accordance with corporate needs, including legal, regulatory, and contractual constraints. Third is sensitive data in public cloud providers, refers to control and restrict how much private or regulated data are stored by public cloud companies. Fourth is cloud access point, refers to how Cloud uses Points for border protection and monitoring tasks that let users use the cloud while shielding the company from it. Fifth is side channel attack prevention, refers to take information out of a chip or system. Figure 5 illustrates Cloud computing as a cybersecurity solution.

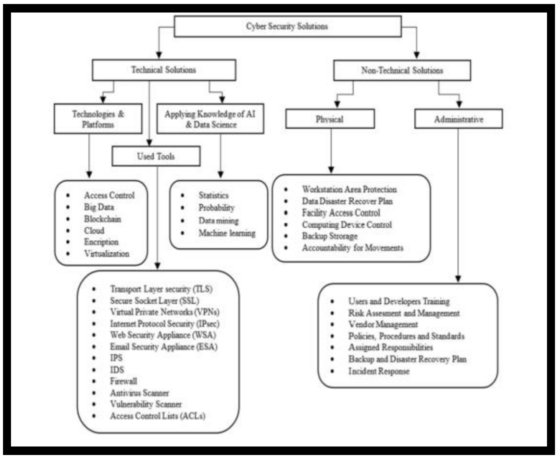
Cyber Security Solutions
Technical Solutions
Non-Technical Solutions
Technologies & Platforms
Applying Knowledge of AI & Data Science
Used Tools
Physical
Administrative
Access Control
Big Data
Blockchain
Cloud
Encription
Virtualization
Statistics
Probability
Data mining
Machine learning
Workstation Area Protection
Data Disaster Recover Plan
Facility Access Control
Computing Device Control
Backup Strorage
Accountability for Movements
Transport Layer security (TLS)
Secure Socket Layer (SSL)
Virtual Private Networks (VPNs)
Internet Protocol Security (IPsec)
Web Security Appliance (WSA)
Email Security Appliance (ESA)
IPS
IDS
Firewall
Antivirus Scanner
Vulnerability Scanner
Access Control Lists (ACLs)
Users and Developers Training
Risk Assesment and Management
Vendor Management
Policies, Procedures and Standards
Assigned Responsibilities
Backup and Disaster Recovery Plan
Incident Response

Figure 5 : Cloud computing as a cybersecurity solutions [28]

21. Maintenance

Other parties, such as maintainers or third-party providers during maintenance activities, can pose a threat related to cyberspace. This can involve malevolent physical entry brought about by exposed infrastructure. The problems may be the result of organizational factors like a lack of awareness and culture surrounding security or an ineffective system for reviewing maintenance tasks. Lack of training among signalers may also contribute to these problems remaining unreported, as several previous occurrences have shown. Problems with abilities, drives, and consciousness may contribute to cyber-threats, not just from maintenance mistakes but also from possible physical assaults. One of the most important elements in determining whether a threat is malicious or not is the level of access that specific parties (such third-party suppliers) may have.[29] It consists of two functions and ten controls. First function is Detect, which contains three controls. First is auditing remote maintenance, which examines the maintenance activity, carried out during remote maintenance sessions and to audit remote, non-local maintenance and diagnostic sessions. Second controls are maintenance validation, which verifies that security measures are in place and that maintenance tasks were carried out correctly in accordance with the work order. Third controls are maintenance monitoring, which gathers, organizes, and reviews audit logs of incidents that may be useful in identifying, comprehending, or countering an attack. Protect is the second function and has seven controls. The first control of maintenance activity is automated maintenance, which uses automated techniques specified by the business to plan, carry out, and document system maintenance, repairs, and replacements. Second controls are timely maintenance, which gets replacement parts and maintenance help for systems within a specified recovery time objective (RTO). Third controls are preventative maintenance, which refers to the routine maintenance tasks that are arranged in advance with the goal of averting future unplanned malfunctions. Fourth controls are automated support for predictive maintenance, which utilizes automated processes set by the company, transfer predictive maintenance data to a maintenance management system. The sixth control is media scanning, which means that there are procedures in place to look for harmful code before employing media that include diagnostic and testing software. Seventh control is remote maintenance notifications and cryptographic protection, refers to safeguard the integrity and privacy of distant, non-local maintenance and diagnostic communications, mechanisms are in place to approve, oversee, and monitor maintenance and encryption operations. Eighth controls are off-site maintenance, which covers all sorts of maintenance of any system component, including applications carried out by a local or nonvocal business, and it deals with the information security implications of off-site system maintenance.

22. Risk Management

The process of risk management involves identifying potential sources of damage or disclosure of assets, weighing those variables against the cost of countermeasures and the value of the asset, and putting cost-effective mitigation or reduction strategies into action. To minimize risk to a manageable level is the main objective of risk management. The process of achieving risk management is known as risk analysis/assessment, which include inventorying assets, scanning the environment for risks, and estimating the likelihood and cost of each risk's occurrence. Figure 6 illustrates the cyclical relationships of risk elements.

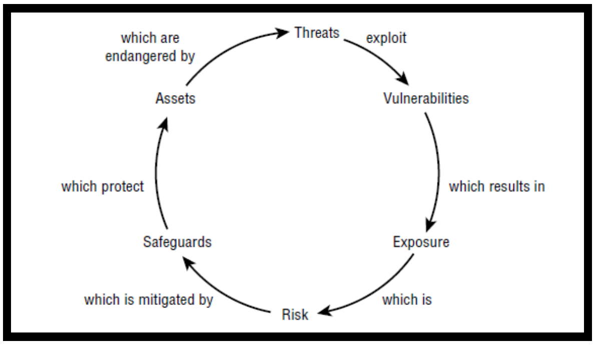

Figure 6 : The cyclical relationships of risk elements [30]

This domain is consisting of four functions and fifteen Controls. First function is Detect, which contains one control, that is Risk Monitoring, which refers to that There are safeguards in place to guarantee that risk monitoring is a crucial component of the continuous monitoring approach, which also entails compliance, change management, and cybersecurity and data privacy control effectiveness monitoring. Second function is Protect, which contains three controls. First is risk management resourcing referring to methods in place to lessen the severity or chance of such effects by allocating the necessary resources to manage technology-related risks. Second is Risk Catalog, refers to that there are procedures in place to create and maintain an inventory of relevant risks related to the company's business activities and deployed technology. Third is AI and Autonomous Technologies Supply Chain Impacts, refers to There are mechanisms in place to handle the risks and advantages associated with Autonomous Technologies (AAT) and Artificial Intelligence (AI) that arise from the organization's supply chain, including data and software from third parties. Third function is Respond which contains one control that is Compensating countermeasures, refers to There are systems in place to recognize and put compensatory countermeasures in place to lessen risk and exposure to threats. Fourth function is Identify which contains ten controls, first is Risk Tolerance and Risk Culture, refers to organizational risk tolerance is defined by mechanisms that specify the acceptable range of outcomes. There are procedures to sure those groups are dedicated to a culture that takes technology-related risk into account and shares it with others. Second is Risk Threshold, refers to organizational risk thresholds, or the degree of risk exposure at which risks are addressed and below which risks may be allowed, are defined by mechanisms. Third is Risk Appetite, refers to organizational risk appetite, or the amount of uncertainty organization is ready to take on in exchange for a return, and is defined by mechanisms. Fourth is Risk Identification, refers to recognize and record risks, both internal and external. Fifth is Risk Assessment and update, refers to procedures in place for routinely conducting frequent risk assessments and updates. It takes into account the possibility and severity of harm from unauthorized use, access, disclosure, disruption, modification, or destruction of the company's systems and data. These procedures also include responding to new risks and security vulnerabilities that are discovered, while gathering information about security vulnerabilities from outside sources. Sixth is Risk Register and Risk Ranking, refers to keep a risk registry updated, which makes it easier to track and report risks. There are methods for classifying recently found security vulnerabilities according to industry-accepted norms and assigning a risk score. Seventh is Risk Response and Risk Remediation, refers to There are procedures in place to address conclusions drawn from audits, incidents, and cybersecurity and data privacy assessments to guarantee that the necessary corrections have been made. There are systems in place to reduce risks to a manageable level. Eighth is Business Impact Analysis (BIA), refers to procedures for doing a Business Impact Analysis (BIA) to determine and evaluate the risks related to data protection and cybersecurity. Ninth is Data Protection Impact Assessment (DPIA), refers to detecting and addressing reasonably foreseeable risks, with mechanisms in place to conduct a Data Protection Impact Assessment (DPIA) of systems, applications and services that store, process and transmits personal data. (PD). Tenth is Supply Chain Risk Assessment, refers to Supply Chain Risk Management (SCRM) plans outline system creation, purchase, maintenance, disposal, mitigation measures, and performance tracking, with regular evaluation procedures for services, components, and systems.

23. Conclusion

Based on the above, it is assumed that the cybersecurity framework will help protect the organizations' assets from security risks in the petroleum industry, in general and in Egypt in particular, as well as their position and ability to successfully complete their tasks. To achieve maximum benefits, this recommended framework is being implemented in more industries. The suggested cybersecurity framework has numerous benefits, the first of which is its capacity to align and integrate various cybersecurity and data protection frameworks and standards. Secondly, offering a cohesive set of guidelines, specifications, and best practices that improve productivity, cut down on redundancies, and enable wiser use of resources. Third, gives enterprises the ability to fully monitor risks, discover access, and fix any vulnerabilities that could exist across several standards and frameworks. Fourth, make sure that cybersecurity and data protection rules are implemented consistently. This is important for keeping a robust security posture and proving compliance with different standards when conducting compliance assessments. Fifth, makes it possible for auditors to adopt an organized and comprehensive strategy, which leads to more successful audits and assessments and minimizes the time and effort needed to evaluate compliance with. Sixth, focuses on a complete set of rules and regulations, allowing businesses to optimize resources. This is particularly helpful for resource-constrained enterprises. The seventh is flexibility, which is achieved by offering a single framework that can adapt to modifications in specific standards. This guarantees that companies stay in compliance with changing rules and regulations. Eighth, facilitating the incorporation of cybersecurity practices into a company's overarching business plan and encouraging a more planned and proactive approach to security. The ninth is ongoing upgrading and development to take into account modifications to the regulatory landscape, technology, and threat landscape. This guarantees that cybersecurity and data protection procedures continue to be applicable and efficient throughout time. Tenth, improved communication between all stakeholders inside the company to guarantee that everyone is pursuing the same cybersecurity goals.

24. Reference

[1] "A Survey of Security Challenges in Cloud-Based SCADA Systems," ***MDPI***., vol. 13, no. 4, p. 19, 2024, doi: https://doi.org/10.3390/computers13040097.

[2] Oladapo Adeboye Popoola, Michael Oladipo Akinsanya, Godwin Nzeako, Excel G Chukwurah, and Chukwuekem David Okeke, "Exploring theoretical constructs of cybersecurity awareness and training programs: comparative analysis of African and U.S. Initiatives," ***Int. J. Appl. Res. Soc. Sci***., vol. 6, no. 5, pp. 819–827, 2024, doi: 10.51594/ijarss.v6i5.1104.

[3] H. Taherdoost, "Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview," ***Electron***., vol. 11, no. 14, 2022, doi:

10.3390/electronics11142181.

[4] H. M. Melaku, “A Dynamic and Adaptive Cybersecurity Governance Framework,” ***J. Cybersecurity Priv***., vol. 3, no. 3, pp. 327–350, 2023, doi: 10.3390/jcp3030017.

[5] T. Y. Khaw, A. Amran, and A. P. Teoh, “Building a thematic framework of cybersecurity: a systematic literature review approach,” ***J. Syst. Inf. Technol***., no. 2022, 2024, doi: 10.1108/JSIT-07-2023-0132.

[6] Oluwatosin Ilori, Nelly Tochi Nwosu, and Henry Nwapali Ndidi Naiho, “A comprehensive review of it governance: effective implementation of COBIT and ITIL frameworks in financial institutions,” ***Comput. Sci. IT Res. J***., vol. 5, no. 6, pp. 1391–1407, 2024, doi: 10.51594/csitrj.v5i6.1224.

[7] K. Kepuska and M. Tomasevic, “A lightweight framework for cyber risk management in Western Balkan higher education institutions,” ***PeerJ Comput. Sci***., vol. 10, p. e1958, 2024, doi: 10.7717/peerj-cs.1958.

[8] M. O. Akinsanya, C. C. Ekechi, and C. D. Okeke, “THE EVOLUTION OF CYBER RESILIENCE FRAMEWORKS IN NETWORK SECURITY : A CONCEPTUAL ANALYSIS,” vol. 5, no. 4, pp. 926–949, 2024, doi: 10.51594/**csitrj**.v5i4.1081.

[9] M. Toussaint, S. Krima, and H. Panetto, “Industry 4.0 data security: A cybersecurity frameworks review,” ***J. Ind. Inf. Integr***., vol. 39, no. March, 2024, doi: 10.1016/j.jii.2024.100604.

[10] M. Neri, F. Niccolini, and L. Martino, “Organizational cybersecurity readiness in the ICT sector: a quanti-qualitative assessment,” ***Inf. Comput. Secur***., vol. 32, no. 1, pp. 38–52, 2024, doi: 10.1108/ICS-05-2023-0084.

[11] N. Mpekoa, “An Analysis of Cybersecurity Architectures,” *Int. Conf. Cyber Warf. Secur.*, vol. 19, no. 1, pp. 200–207, 2024, doi: 10.34190/iccws.19.1.2115.

[12] B. Riskhan, A. M. Raufi, and M. Hamza, “Physical Security to Cybersecurity (Challenges and Implications in the Modern Digital Landscape),” **J. Electrical Systems** .,vol. 20, no. 4s, pp. 692–702, 2024, [Online]. Available: https://www.proquest.com/openview/750732a0466f074418d548fe19b79734/1?pq-origsite=gscholar&cbl=4433095

[13] A. Kumar, M. Fahad, H. Arif, and H. K. Hussain, “Advancements in Detection and Mitigation : Fortifying Against APTs - A

Comprehensive Review," **Multidisiplin Ilmu**., vol. 3, no. 01, pp. 141–150, 2023, [Online]. Available: https://journal.mediapublikasi.id/index.php/bullet %7C

[14] D. Bringhenti, G. Marchetto, R. Sisto, and F. Valenza, "Automation for Network Security Configuration: State of the Art and Research Trends," ***ACM Comput. Surv***., vol. 56, no. 3, 2023, doi: 10.1145/3616401.

[15] H. Doshi, ***Certified Information Systems Auditor Study Guide***, ***Second edion***., vol. 1, no. 15. 2020. [Online]. Available: https://www.amazon.com/CISA-Certified-Information-Systems-information/dp/1838989587

[16] C. Information and S. Manager, ***CISM ® Certified Information Security Manager E X A M G U I D E Second Edition***, Second edi. United States: McGraw Hill, 2023. [Online]. Available: https://z-lib.io/book/13540237

[17] M. Waddell, "Human factors in cybersecurity: Designing an effective cybersecurity education program for healthcare staff," ***Healthc. Manag. Forum***, vol. 37, no. 1, pp. 13–16, 2024, doi: 10.1177/08404704231196137.

[18] U. Mmaduekwe and E. Mmaduekwe, "Cybersecurity and Cryptography : The New Era of Quantum Computing," **Current Journal of Applied Science and Technology.,** vol. 43, no. 5, pp. 41–51, 2024, doi: 10.9734/CJAST/2024/v43i54377.

[19] James Olakunle Oladipo, Chinwe Chinazo Okoye, Oluwafumi Adijat Elufioye, Titiola Falaiye, and Ekene Ezinwa Nwankwo, "Human factors in cybersecurity: Navigating the fintech landscape," ***Int. J. Sci. Res. Arch***., vol. 11, no. 1, pp. 1959–1967, 2024, doi: 10.30574/ijsra.2024.11.1.0258.

[20] D. Van Tran, P. V. Nguyen, L. P. Le, and S. T. N. Nguyen, "From awareness to behaviour: understanding cybersecurity compliance in Vietnam," ***Int. J. Organ. Anal***., 2024, doi: 10.1108/IJOA-12-2023-4147.

[21] G. Stamenkov, "Cloud service models, business continuity and disaster recovery plans, and responsibilities," ***Int. J. Organ. Anal***., vol. ahead-of-p, 2024, doi: 10.1108/ijoa-12-2023-4127.

[22] M. D. Elradi, K. A. Abdelmaged, and M. O. Mohammad, "Cyber Security Professionals' Challenges: A Proposed Integrated Platform Solution," ***Electr. Sci. Eng***., vol. 3, no. 2, pp. 1–6, 2021, doi: 10.30564/ese.v3i2.3376.

[23] M. S. Ahmad and H. V, “The Role of Threat Intelligence in Enhancing Cybersecurity Posture,” ***Int. J. Innov. Res. Comput. Commun. Eng***., vol. 12, no. 03, pp. 1739–1746, 2024, doi: 10.15680/ijircce.2024.1203061.

[24] A. Naseer, H. Naseer, A. Ahmad, S. B. Maynard, and A. M. Siddiqui, “Moving towards agile cybersecurity incident response: A case study exploring the enabling role of big data analytics-embedded dynamic capabilities,” ***Comput. Secur***., vol. 135, no. October 2022, p. 103525, 2023, doi: 10.1016/j.cose.2023.103525.

[25] M. Thakur, “Cyber Security Threats and Counter Measures in Digital Age,” ***J. Appl. Sci. Educ***., vol. 04, no. 042, pp. 1–20, 2024, [Online]. Available: https://doi.org/10.54060/a2zjournals.jase.42http://creativecommons.org/licenses/by/4.0/

[26] Temitayo Oluwaseun Abrahams, Oluwatoyin Ajoke Farayola, Simon Kaggwa, Prisca Ugomma Uwaoma, Azeez Olanipekun Hassan, and Samuel Onimisi Dawodu, “Reviewing Third-Party Risk Management: Best Practices in Accounting and Cybersecurity for Superannuation Organizations,” ***Financ. Account. Res. J***., vol. 6, no. 1, pp. 21–39, 2024, doi: 10.51594/farj.v6i1.706.

[27] A. I. Mallick and R. Nath, “Navigating the Cyber security Landscape: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and Recent Developments,” *Int. Conf. Cyber Confl.*, no. February, 2023, [Online]. Available: www.worldscientificnews.com

[28] F. Jimmy, “Cyber security Vulnerabilities and Remediation Through Cloud Security Tools,” ***J. Artif. Intell. Gen. Sci***. *ISSN3006-4023*, vol. 3, no. 1, pp. 196–233, 2024, doi: 10.60087/jaigs.vol03.issue01.p233.

[29] E. Thron, S. Faily, H. Dogan, and M. Freer, “Human factors and cyber-security risks on the railway – the critical role played by signalling operations,” ***Inf. Comput. Secur***., vol. 32, no. 2, pp. 236–263, 2024, doi: 10.1108/ICS-05-2023-0078.

[30] S. D. G. Mike Chapple , James Michael, “**CISSP Certified Information Systems Security Professional Official Study Guide 9 Edition**,” *Pap. Knowl. . Towar. a Media Hist. Doc.*, pp. 12–26, 2020, [Online]. Available: https://www.amazon.com/Certified-Information-Security-Professional-Official/dp/1119786231