Journal Homepage: - www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI: 10.21474/IJAR01/15433
DOI URL: http://dx.doi.org/10.21474/IJAR01/15433

RESEARCH ARTICLE

DYNAMIC RISK ASSESSMENT FOR CRITICAL INFRASTRUCTURES UNDER ATTACK

Blondel Seumo Ntsiepdjap
Ph.D. in Cyber Security Administration.

Manuscript Info

Manuscript History
Received: 25 July 2022
Final Accepted: 28 August 2022
Published: September 2022

Abstract

Concerns in regards to enterprises are cyber security threats and their associated problems. Kostayeva and Chemyakov (2020) stated that digitalization and breathtaking techniques had escalated these cyber-related risks. As time progresses, commercial enterprises become cognizant and take action against cyber risk. For this reason, they are finding strategies to cope with management and data safeguards. A fundament challenge in business being encountered is appropriate and adequate data from online crooks.

Copy Right, IJAR, 2022,. All rights reserved.

Introduction:-

Background

Concerns in regards to enterprises are cyber security threats and their associated problems. Kostayeva and Chemyakov (2020) stated that digitalization and breathtaking techniques had escalated these cyber-related risks. As time progresses, commercial enterprises become cognizant and take action against cyber risk. For this reason, they are finding strategies to cope with management and data safeguard. Fundament challenge in business being encountered is appropriate and adequate data from online crooks.

It has been observed that efficient risk evaluation strategies are the foundation for a prosperous security program concerning Critical frameworks. This statement is endorsed by a considerable amount of methodologies associated with evaluating risk for critical Infrastructure. Evaluation of threat provides a vital role for threat recognition, estimation of susceptibilities, resources influence estimation, and effect on infrastructures with the intent to investigate the possibility of the threat exists.

Role of European nations in risk assessment

Assessment (2010) stated risk coupled with disaster management by European commissions. In order to do so, the European Commission provided recommendations for the evaluation of threats to assist MS (Member states). Likewise, the European Commission (2014) stated the outline for risks of natural and synthetic ones after reporting recommendations and donations by Member states. Loss of critical structures has been recognized among several results of risk assessment. Result level indicators are employed, which helps determine the degree of project accomplishment. In the study, the loss of vital services acts as an impact indicator to comprehend critical infrastructure risk evaluation. Directive (2008) study has pinpointed the significance of critical infrastructure risk evaluation at the European level. However, risk assessment strategy is not associated with a critical framework since Member states pursue strategies to combat issues. It has been observed that several cross-sections, such as financial and public influences and causalities, function as the essential foundations for the evaluation of risk impact. However, Member states (MS) still have not embraced a specific approach for evaluating critical structures associated with threats. It suggests that it is not convenient to find the comparison among Member states' risk

Corresponding Author:- Blondel Seumo Ntsiepdjap
Address:- MBA in Information Technology (Singhania University - 2021).

assessment outcomes. Based on national outcomes, multi-risk and cross border evaluations also have been predicted. In addition, the Directive is employed in Energy and Transport sectors owing to the range of scope across the sectors. As a result, this does not permit the evaluation of all essential services offered by Critical infrastructures.

Udeanu (2015) presented a document of commission active personnel that reflects upon a novel strategy for protecting critical infrastructures with the aid of European programs. This, in turn, offers protection to critical European Infrastructure. It elaborates the introductory step of commission for the approaches coupled with risk evaluation under the influence of the CIPS program. Assessment (2010) elaborated that DG-ECHO guidelines target documents that elaborate sectoral approaches during the resolution of cross-sectoral risks. These approaches deal with collaborative work and critical European infrastructures that include gas emission networking, the transmission of the electricity grid, Eurocontrol, and Galileo. It has made advancements in system strategies.

The advancement in the evaluation of risk involves four pilots. Besides, threatening risk management approaches to deal with minimal to maximum possibilities. These strategies could be employed in the prospective future with the help of stress tests for critical infrastructure evaluation, as elaborated by Galbusera et al. (2014). Global risk report in 2015 has mentioned economic work forum that identifies critical information for infrastructure malfunctioning. This is the joint combination of hyper-connectivity reported patterns linked to threats associated with technologies in which critical infrastructure loss is included. It is suggested that critical infrastructure associated threat evaluation tends to be employed in segregation. In numerous instances, a cause and effect association has been observed among them due to the mutual sharing of vulnerabilities. It has raised numerous queries linking to multi-risk strategies due to intricacies in risk addressing and probabilities of potent outcomes. However, it also has prepared at several levels, such as local, national, regional, and global.

Role of European nations

European Union has targeted the improvement of resilience ability and protection to deal with critical infrastructure (CI) hazard influences. It has been found that vulnerabilities towards predictable and unpredictable threats have risen to a greater extent. The study aimed to confine the possibility of substantial ranged negative influences on citizens of European nations and their financial status. For this, the Stockholm program was introduced by Council (2010). Besides, the European internal security strategy was elaborated by Horjan and Šuperina (2012).

Carpignano et al. (2020) described resilience based on UNISDR (United Nations International Strategy for Disaster Reduction). Resilience includes system /community/society capabilities to resist threats to reconstruct fundamental functions. This definition could be employed in the context of critical infrastructures. In 2004, the EU commission presented resilience as a protection of a critical framework in the fight against terrorism. It has been noticed that critical Infrastructure (CI) is the indispensable structure in the context of networking, resources, and facilities. However, its disorganization leads to a suitable influence on Member states (MS) advancement and social & economic circumstances. In addition, to safeguard against unlawful violence and intimidation, it also protects against numerous potential risks in conjunction with natural disasters as elaborated by the EU commission (2005) EU commission (2006) under EPCIP (European Programme for critical infrastructure protection). This program was targeted to elaborate the basic framework based on numerous principles that comprise shareholders' collaboration, confidentiality, sector-based strategies, subsidiary, and proportionality. EU Commission (2005) emphasized ECI (critical European Infrastructure), which describes the location of the critical Infrastructure in Member states of European Unions, and disruption could lead to impact considerably two Member states. Besides, probabilistic mutual reliance, threat evaluation with several strategies, and safeguard improvisation measurements are presented. Moreover, the European Union was influenced due to hazardous incidents out the European border and contingency plan with the intent to decline critical infrastructure disruption effect as stated by EU Commission (2005)

EU union (2008) has elaborated that the 2008 directive was considered one of the best documents being created for ECIP execution. It describes European critical infrastructure recognition with specifications targeted to evaluate risk with the intent to offer safety. It describes the first strategy for recognition of ECI to enhance the safety measures. Moreover, it was ascribed to the energy and transport sectors only while emphasis is given to other sectors such as information and communication technology (ICT) in the future. Moreover, OSP (operator security plan) is introduced to elaborate on several existing or executed choices related to the protection of ECI. For the creation of OSP plans, operators are required. Udeanu (2015) has elaborated on the EPCIP revision. This revision was being targeted for activities execution in addition to workstreams such as preparedness, prevention, and response for

strengthening the mutual dependencies between cross-sector and cross the border after appropriate analysis. Furthermore, ICT infrastructure and its association with transmission infrastructure and electricity generation were included.

European Commission (2017) has commenced the 2008 Directive assessment and evaluation by including effectiveness, coherence, relevance, sustainability, and EU added values. This holistic evaluation was accomplished in the year 2019. It imposes the necessity on revised Directive proofs which comprise various other sectors apart from transport and energy by including mutual dependencies between these sectors. In addition, the European Commission (2008) pinpointed the significance of novel concerns about artificial intelligence. Advancement in ICT Resolution reflected upon novel insecurities, adoption of third nation's ownerships, and critical infrastructure operations.

For enhancement in critical infrastructure protection, there are several quantitative approaches designed that help to assess resilience based on an integrated approach, including several aspects.In literature, several strategies are being suggested that emphasize various prime fundamentals associated with framework resilience concepts, such as ad hoc risk strategies for critical infrastructure resilience quantification, critical infrastructures mutual connections, and framework susceptibility analysis regarding various other concerns. In addition to this, the multidimensional influence of social, energy, economic, and environment owing to Critical Infrastructure coupled with catastrophic events.

Ouyang (2014), Griot (2010), Wang (2011), and Liu and Song (2020) studies reflected upon various investigations associated with multidimensional aspects. By considering these several approaches of quantitative nature with the intent to assess the resilience of the critical Infrastructure, JRC has described two studies. Specifically, Galbusera et al. (2014) have projected the feasibility analysis in the form of stress tests in order to measure critical infrastructure resilience assessment for combating various threats. These tests are similar to the test adopted in the economy and nuclear.

Giannopoulos et al. (2012) have described the modern analysis of evaluating threats to safeguard the critical infrastructures. Likewise, some authors have elaborated several strategies for risk management and analysis. Haimes (2008), Pinto et al. (2012) Eusgeld et al. (2011) has suggested HLA (High-level architecture) for several application such as SCADA(Supervisory Control and Data acquisition) and Suc(System Under control)Haimes(2008) and Pinto et al., (2012) stated that risk management and its analysis for the system of the system (SOS) is conducted with the assistance of a comprehensive strategy.

Eusgeld et al. (2011) study has suggested HLA (High-level Architecture) for SuC(System under control) and SCADA(Supervisory Control and Data acquisition). This study was based on analysis rather than integrated and coupled model options. A comprehensive system relies on resilience policy recognition, impacts, and execution methodology. This system was recommended by Labaka et al. (2015) and Labaka et al. (2016), which is meant to be targeted for enhancement in critical infrastructures resilience with the aid of resilience level recognition, fragility, and probable improvisation for execution.

Mao et al. (2019) have pinpointed several measurements to enhance the resilience of the critical Infrastructure as CI were combating each other owning to lacking in systemic methodology. For that reason, a structure coupled with QFD (Quality function deployment) has been framed, which includes the interrelationship of resilient performances on various levels of critical infrastructure life span. Nan and Sansavini (2017) considered a strategy for evaluating resilience that is the joint combination of integrated metric and hybrid multilayer model. Integrated metrics were employed for resilience quantification with various resilience capacities. A hybrid multilayer model was made for various subsystem interactions. Quyang et al. (2019) highlighted safeguards actions for critical infrastructures before catastrophic events. For this, robustness and resilience-based strategy were used. Robustness deal with system practicality level, and the resilience approach comprises probable routes for restoration and quickness.

Critical Infrastructure and Risk management

Several authors have described mutual reliance owning to the interconnection between the system (SOS) of Infrastructure. Theocharidou and Giannopoulos (2015) have evaluated CRISRRM(critical Infrastructure, systems risks, and Resilience assessment methodology)due to the SOS approach as defined by Choi et al. (2007) that presented assets, system, and Society intending to assess the influence on residents, environment, and economy in

direct or indirect ways especially, due to various dangers. Moreover, Monte Carlo simulation and Hierarchical Graph presentation related to critical infrastructure freedom are elaborated by Ferrario et al. (2016). This paper assessed robustness based on two cases such as SCADA (small electric and gas grids) and large electrical network distribution. Furthermore, Kröger and Zio (2011) and Zio (2016) recommended a strategy based on concepts coupled with vulnerabilities and risk for critical infrastructure safeguards. It would permit the recognition of both insecure and apparent susceptibleness to prevent collapse, which could arise due to hazardous impact on critical infrastructures.

Johansson et al. (2013) highlighted an analysis of susceptibilities linked to accomplishing critical infrastructure-based trustworthiness investigations. It has been showcased with Monte Carlo strategies and Vulnerability analysis for reliability and electric power system evaluation, respectively. In addition, Johansson and Hassel (2010) have suggested a model for interconnected structures susceptibility analysis. These structures are elaborated based on the functional model and graph theory. Stergiopoulos et al. (2015) have examined critical infrastructures in mutual reliance that generate ripple influence in the event of default. Kotzanikolaou et al. (2013) suggested a dependency risk approach and presented graph metrics with the intent to recognize nodes and precarious affection paths. This, in turn, could be utilized for threat regulation and elimination.

Moreover, Stergiopoulos et al. (2016) have protracted the research conducted by Kotzanikolaou et al. (2013) after the inclusion of temporal changes noticed by the fuzzy model and synchronous collective objectives associated with failures. It led to the emergence of CIDA (critical infrastructure Dependency analysis) associated equipment for the decision process. These pieces of equipment are proven to be worthwhile in measuring critical infrastructure endurance underneath several situations and probabilistic alleviation actions. On the one hand, Fu et al. (2012) have pinpointed addressing structures networking as interconnected sos (system of the system). While on the other hand, Utne et al. (2011) have suggested methodological strategies for modelling critical Infrastructure's mutual dependencies from the simple cascade diagrams. In addition to that, Azzini and Dido (2016) have stated that GRASP (Geospatial Risk and Resilience Assessment platform) act as graphical equipment, which could be employed to analyze networking system to recognize the critical elements and evaluation of the effect on critical infrastructures disruptions by including the cross border mutual dependencies and cross-sectoral.

Rationale

In the contemporary world, a considerable concern being faced by corporate enterprises is the safeguard of essential knowledge regarding clients, enterprises, and employees. The primary purpose of the investigation is associated with the alleviation of threats owing to the implementation of digitalization techniques and pieces of equipment. It has been noticed that the dispersion of cyber risk occurs similar to the web in order to generate susceptible scenarios for each enterprise. However, Cappiello (2010) has analyzed all the concerns thoroughly with the intent to offer suggestions that could be employed to avoid situation threats.

Aim

The prime target of this investigation dealing with strengthening the cyber threat concerns the utilization of efficient digitalization tools.

Objective:-

1. To recognize the factors that reinforce the cyber risk concerns.
2. To comprehend the efficient usage and the adequate digitized tools for reducing cyber threats.
3. To enhance the efficiency of digitalized tools in the management of the cyber threat in management of enterprise
4. To suggest strategies to alleviate the cyber risk concerns associated with digitization
5. 1.5. Research Questions
6. How do we recognize the factors to reinforce the cyber risk concerns?
7. How do we comprehend the efficient usage of digitalized tools for declining cyber threats?
8. How do we enhance the efficiency of digitalized tools in managing cyber threats in enterprise management?
9. How to suggest strategies to alleviate the cyber risk concerns associated with digitalization?

Scope of research

The prime relevance of the investigation is the alleviation of cyber threat concerns management and its enterprise management. In addition, the investigation's main scope involves identifying all the concerns and obstacles to cyber

threats incorporate organizations. Besides, the investigation would offer all the digitalized resources to mitigate obstacles coupled with cyber risk. In the study, a dynamic risk assessment would be utilized to evaluate threats. Several applications have been noticed by comprehending the path of dynamic risk evaluation.

1. It would help to take a proactive strategy for the intent of safety aspect. This, in turn, offers knowledge related to risks and hazards in various scenarios
2. For the assessment of an adequate environment for gaining confidence. Since adequate training is needed for instant observation, analysis, and hazardous
3. After getting safety, it becomes feasible to conduct work confidently and adapt to unpredictable scenarios.

Chapter 2: Literature Review

Concept of digitalization

Digitalization is employed to elaborate the techniques linked to the digital area with the aid of enterprises. It leads to alteration and offers novel value-productive probabilities in the refinement and the advancement of enterprises coupled with the digital area. Execution of Digitalization in enterprises endorses the improvement of effectiveness in various core business activities, steadiness, and quality, as elaborated by Vartolomei and Avasilcai (2019). Thus, it is associated with combining all the traditional documentation in audit associates for eradication of all concerns coupled with communication series.

The digitalization in case studies

To address the constantly blossoming need for betterment and improvisation of services with the purpose of interacting with the presumption of the clients in the private and public sectors. Several authors have several digitalization and smart cities as introductory steps, as stated by Bakıcı et al. (2013), Denhardt and Denhardt (2015), and Taylor Buck and While (2017). In the study, both have been thoroughly included. The first case was associated with programs linked to smart cities, their presentation, and their execution with the intent to offer several facilities in the public administration area employing several investigations in assisting the cities. The prime purpose of research or trial was to investigate the sprouting innovations that could be executed and widespread to offer permanent services linked to the city's executive for strengthening the city dweller's life.

Hellsten and Pekkola (2019) stated that the subordinate objective for the examination leads to the formulation of a positive attitude inclined toward digitalization. In addition, open web resources permit digital benefits regarding fabrication and Infrastructure associated.Helanderet al. (2019) stated that in Finland, the Ministry of Finance had elaborated facilities formulation in the SADe program (eServices and e-Democracy). This program was designed to offer inter-operating and prime quality facilities linked to prime quality with the help of digital means to establish economic effectiveness and savings. It would be worthwhile not merely for city dwellers and big enterprises but offers benefits to government and local administrations. It has been noticed that the Digi program was an integral part of smart city as an introductory step. The city's top management has devised a big introductory step in which CIO was the member. Therefore, the Digi program has emerged from the CIO office in the city. In this case, an essential foundation is created due to the assignment of the program manager and several CIO office staff members. However, the prime emphasis lies in other places, such as service areas.

It has been presumed that several service executives are found to offer eagerness. However, few provide the least availability for contribution in the introductory step. Digi program is obliged to have several staff members of the particular area who function as project managers. On the other hand, several people act as supportive managers for the development. In addition, there are steering groups consisting of high-level advisors being assigned to offer an appropriate path to specific projects or organizations. These group members were employed to supervise and direct the efforts in numerous services. This program has included several services categories coupled with city public administration. The trial concepts have emerged from numerous service categories. Since it has been thoroughly understood the mechanism of digitalization to endorse the people, Hellsten and Pekkola(2019) stated that experiment objectives are associated with the investigation if, in case, service innovations could be executed to execute permanent city administration services. Besides experimentation, the supplementary target for the development is general behaviour that was inclined towards administration growth with the help of digitalization. Based on several factors, experiments being conducted vary. These trials vary based on different shapes and sizes. On the one hand, less eagerness was observed to have efficient regular conferencing by employing e conferencing pieces of equipment, skypes, etcetera. On the other hand, innovative reconsideration leads to the formation of operational new procedures.

City dwellers are associated with professions in service areas such as civil servants. However, there are several exceptions in which some people are inclined towards anticipation in various initiatives over persons engaged in the city's payroll. It is noticed that the attitude towards techniques potential is considered to offer a prime role though these techniques might not be of the highest quality. Another instance of Lupapiste was a web-linked open-source service. This service endorses digitalization applications for construction permits and other permissions of Infrastructure. Ministry of Environment organized Lupapiste as a subproject of many programs. For Lupapiste, Solitainc was being opted to offer service following a competitive process. Helander et al. (2020) elaborated that Lupapiste service is offered by progressive communities that function as Inventors. Subsequently, ownership was shifted to Evolta Inc (a corporate spin-off from Solita Inc) during the growth in services. In the contemporary, Lupapiste(2020) stated that 60 per cent of local authorities of Finland possess 100,000 operators who are utilizing Lupapiste service. During the exploration of these cases, 16 interviews were performed with corporate agents in the field of Urban planning, electric engineering, and architecture. In Finland, interviewees consistently utilize the Lupapiste services for work with the order to execute in several permission linked to architecture, electric engineering, etcetera. It has been observed that the operator's experience was found to be a positive one. Furthermore, application procedures have been observed to show an alleviation effect.

Concept of cyber security

Cyber security deals with the applicability of regulation of the system with the assistance of various techniques. Its procedures involved with programming and networking of appliances in addition to data beyond the internet-based attacks. The prime purpose of cyber security was associated with the decline in the threats of crimes on the internet and safeguards against unscrupulousness authorization related to operational procedures and networkings as suggested by Schauer et al. (2017)

It is considered a prime concern in the framework linked with each institution and corporate setting. In brief, a corporate or institution coupled with computer safety endorses attaining an elevated position and an infinite number of achievements. Since it has been noticed that prosperity emerges as a consequence of corporate competencies with the intent to safeguard private and client-associated information in opposition to contestants. There are numerous institutions and contestants linked with clients and people observed as depreciative. Rodríguez-deArriba et al. (2021) stated that institutions or corporate ought to offer a safeguard in the good sense with the purpose of adequate establishment and development.

Cyber security comprises concrete steps for safeguarding data as opposed to various hazards such as internal or external and protection of networking. Therefore, experts are fundamentally engaged in safeguarding servers, intranet, computer system, and network.Ahmed Jamal et al. (2021)elaborated that cyber security ascertains legitimate people and leads to the accessibility of data. It has become vital to comprehend the several kinds of cyber security for enhancement of safeguard as mentioned in Figure 1

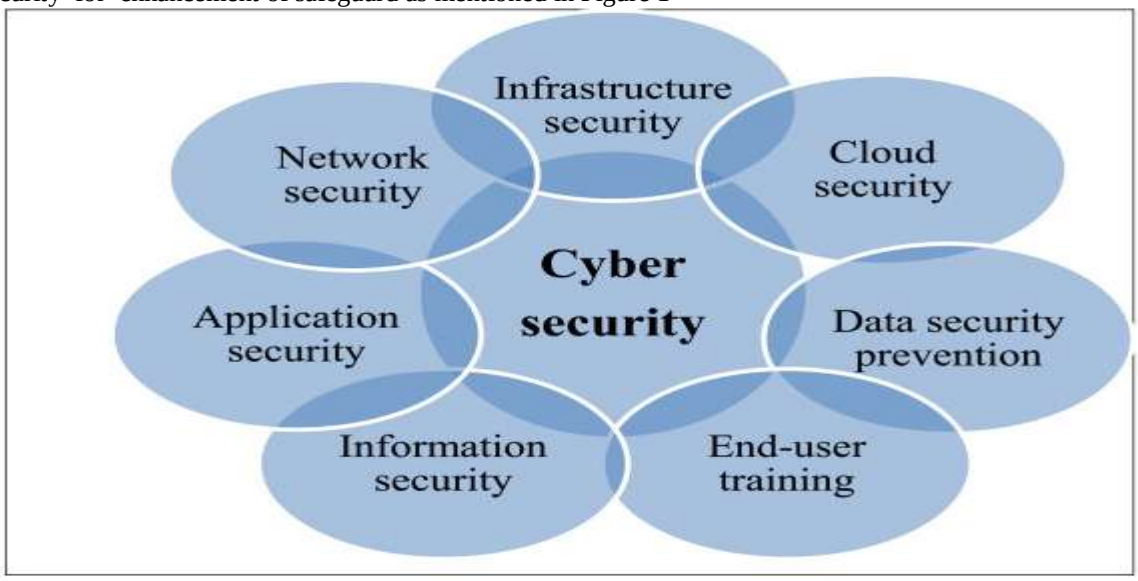

Figure 1:- Security Triangle (CIA).

Following are the various categories of cyber security:

Network security:
Zhang (2021) has stated that the safety of the network leads to guarding against disturbers such as hacking or malware.

Application Safety:
With the aid of several software and hardware programs like encryption, firewalls, and antivirus programs, the computer system is being protected in opposed to dangers that could lead to the interruption in the development of the application, as elaborated by Alkatheiri et al., (2021)

Information Security:
Ogbanufe(2021) has stated that digital and physical information needs to be safeguarded as opposed to illegitimate accessibility, forbidden alterations, elimination, misapplications and et cetera.

Practicable safety:
Ogbanufe(2021) elaborated on the procedures and resolutions that must be utilized to maintain and regulate information. To illustrate, operators' authorization while procedures or networks are retrieved to precisely describe data location, storage, and retrieval.

Cloud safety:
Krishnasamy and Venkatachalam (2021) mentioned that data in software clouds are protected and regulated to eliminate associated internet threats.

Training of operators:
In this case, inconsistent cyber safety associated attribute is discussed. It has been observed that sometimes individuals unintentionally are prone to capture viruses by intruding on system safety. Thus, Krishnasamy and Venkatachalam (2021) show that operators are being taught to eliminate the dubious emails that are not connected to anonymous USB (Universal serial buses) and other critical concerns that ought to be an integral part of the corporate security plan.

Cybercrime is considered an illegitimate authorization was comprising networking, appliances, and system. There are two kinds of cybercrimes elaborated: The first one is associated with the system for the target. The second one has linked the illegal activities conducted by the system unintentionally. Institutional safeguard is emerged based on three fundamental principles –confidentiality, integrity, and availability (Figure 2)

Fig. 2:- Different types of cyber security.

Palmieri et al. (2021) described these three principles as the central intelligence agency (CIA) or security triangle. The aim of these principles is associated with system safeguard. The confidentiality principle elaborated the legitimate access to resources that possess susceptible functions and knowledge. To illustrate, confidentiality deals with Military secrets. As far as the integrity principle is concerned, it elaborates that legitimate people can make alterations in addition to or elimination of susceptible knowledge.

Availability principles asserted that system data and operation ought to be accessed after relying on measurements of SLA service level, as stated by Nguyen and Golman (2021). Practical cyber-security approaches can go beyond the principles elaborated. The advanced ethical hacker could make the alternative path for defending the mechanism. With the growth of corporations, it has become a predicament to maintain cyber-security. In addition to that, another problem coupled with cyber security is the treatment of participants with actual and virtual data information exchange.

Apart from this, another obstacle coupled with cyber security is the insufficiency of an acceptable profession. Several individuals are at the inferior end regarding skills related to cyber security. Scope of cyber security necessities a comprehensive approach that includes various aspects, as stated by Alzubaidi (2021). It has been noted that huge global frameworks act as integrated cyber-physical roles. Humans certainly receive several applications with the assistance of marvellous frameworks.

Nevertheless, the internet-based system employed in these structures poses a cyber threat owing to cyber attacks and illegitimate hacking activities. Therefore, institutions' policymakers must include several things that describe the attack on performance level. It has been founded that novel hackers consider web-based applications as vulnerable spots to being attacked. Top-notch encryption is required for the security of the system.

For this reason, various approaches need to be customized and designed for execution in various enterprises. In similar ways, infiltrating and hacking become less. The various organization ought to pose a security perspective for comprehending cyber security. This, in turn, offers high surveillance assurance owing to a rise in security ventures and investment in enhancing security. Chandra and Snowe (2020) stated that Cisco, McAfee, and Trend Micro companies have high activity in this area.

Policies of Cyber-security

Cyber has enhanced the outcome of Society, which leads to the efficient dissemination of data over time. There are no concerns associated with utilizing the type of application or industry cyber. However, a rise in yield is always taken into consideration. Quick transmission of information to cyberspace leads to a reduction in the average safety of the system. Katrakazas et al. (2020) stated that technology experts are responsible for making improvements in yield and safety indicators which are in confrontation with advancement since prevention indicators help in the reduction and forbidding the operator's access. At the same time, consumer indicators are utilized to recognize critical system resources in reaction to attention offered by management.

It has been observed that alterations in the system cause adequate and instantaneous appliances. There is always combat between security scenarios and requests for cyber output, and the policies associated with cyber security play a vital role. Policy term is utilized across various sectors linked to cyber security, which could be applied to knowledge and the dissemination of several regulations and rules—saving the data in private sectors and various approaches for regulation of technologies. Nevertheless, policies associated with cyber security are utilized in fulfilling diverse objectives. Tam et al. (2021) stated that there is no doubt that the cyberspace phrase has no concrete interpretation like cyber security policies.

The regulatory structure acknowledges the cyber security policies formally requested by the suitable fields of governors. Cheng et al. (2020) stated that policy scope categorizes security policy into different elements. For instance, the national cyber security policy comprises all inhabitants and overseas entrepreneurs engaged in their respective areas. However, a cyber security corporation applies to staff members working with legitimate consent and are presumed to maintain appropriate conduct in corporate settings.

Alghamdi (2021) stated that it is unbelievable to presume support organizations are contingent upon one client with the intent to offer a security policy until a formal agreement is established. Several targets associated with the

suitable regulatory body investigate the security policy content. It has been noticed that company safety-related goals are found to be contrasting with national security objectives.

The policy elaboration and registration pattern concerning the policy will be evaluated due to various institutions, and its acceptance will be measured through several elements and a regulatory board. It has been observed that several procedures are being utilized to design policies. Furthermore, mechanisms through which policies are merged into various legislations vary. However, corporations deal with centralized protection desk, which is found to be accountable for various cyber security policies and associated regulations to find the solution to problems. In a corporation, safety standards and its resolutions direct the regulatory guidance. It has been noticed that whenever an institution offers excellent importance to the safety aspect, then it becomes vital to observe the cyber security policies being delivered with the assistance of several inner units belonging to the standard element section.

Quigley et al. (2015) stated that these essential elements somehow are coupled to recognize discrepancies in various policies under the execution of concerns at the exact moment. In the contemporary era, nations' cyber policy is considered a component of national safety policy, even though nation's safety policies are congruous with economic policies or State Department policy (SDP). However, these policies and legislation are not supreme like the constitution.

Exploration related to several aspects is conducted in order to generate policies to create reports. There are numerous policies generated for offering lead to conclude terms of regulations and legislation. However, policies are not associated with the legislative and regulatory frameworks. In the best scenarios, consents, legislation, and rules illustrate significant and prudent policy. Sakhnini et al. (2021) stated that cyber security implemented rules, regulations, and verdicts could be offered in the absence of cyber security policies.

It has been observed that company settings involve several sections presumed to pursue the orders owning to the insecurity of penalty since penalty leads to the remain till lawless field encloses. To illustrate, individual assets and pricing policies are systemized or written to such a level that refusal to comply with notification rules leads to the closure of the appropriate segment. Intermediate managers endorse the procedures like employee recruitment and administration expenditure. It is presumed to include talkative policies into sectional operations And as generation of measurement at the department stage to evaluate the compliance for policies. Baig et al. (2017) stated that organization subsection of all different kinds encounters significantly limiting factors associated with administration in the public domain.

Various exemptions possess several serious areas related to the classification of knowledge. However, it has been noted that a CEO-created security policy needs to be implemented in a holistic corporation though CEO authorized security policy was confined to a specific area. In recent times, alteration in the spectrum of organizations in terms of work conducted by senior security managers, accountable for various aspects linked to the institution's security scenario. Moreover, unacceptable variation between individual assets or legitimate policies and organization internet-based policies is observed.Arend et al. (2020) showcased that an internet-based security policy might be needed while the threat linked to confidentiality knowledge is relatively higher. Therefore, knowledge ought to be offered without careful thought of receivers' potency to preserve the safety information.

Policy withdraws the evaluation of threats associated with information on managers accountable for a decline in expenditure by contracting out the data rush to administrative offices and outsider individuals to analyze information.Perhaps similar managers are hoping to neglect the safety concerns to decline the expenses. This scenario could be considered the consequence of misjudgment related to data obligations for individuals except for security officers. In each scenario, it is vital to assign several tasks. It is pinpointed that these scenarios become intricate and tedious. For this reason, cyber securities parameters are not found to be fully developed like human assets indicators or accounting.

Conceptual framework

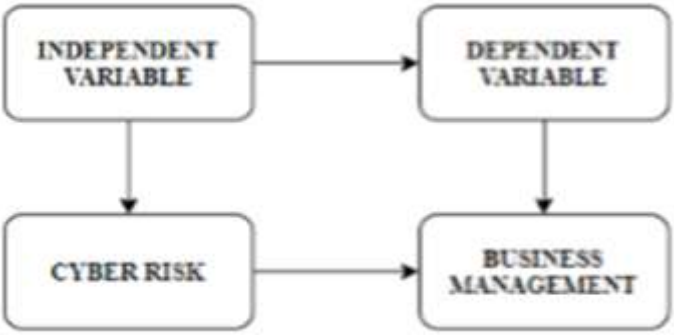

Figure 3:- Conceptual Framework.

Theoretical framework

Active Situational Awareness Model

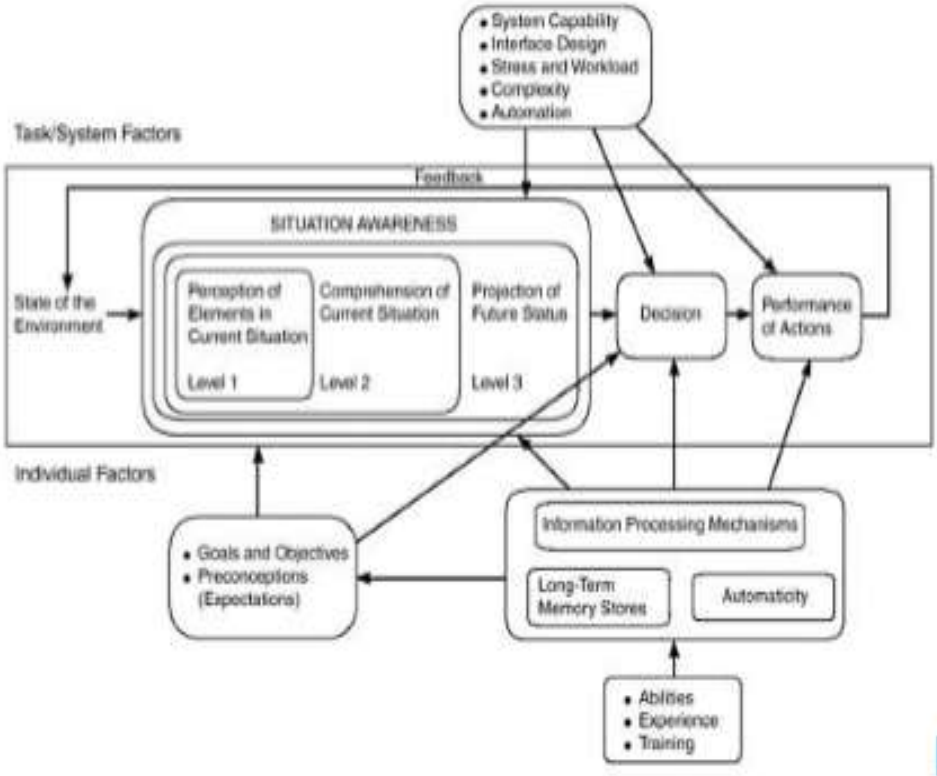

Figure 4:- Generic decision-making model centred on the situation awareness process (Ensley, 1995).

Sheehan et al. (2012)showcased that the situational awareness model works as the active component, presenting several incidents concerning a specific period interval. Thus, it works as a practical model with the intent to identify the effective judgment for corporations in a broad spectrum of specific scenarios.

Cyberthreat enhancement due to Digitalization

Cyber threats fall under a more comprehensive framework than data processes. Information operations deal with combinatorial utilization of prime capacities related to psychological, computer networks, electronic warfare, and security operators. These capabilities are in connection with suitable abilities and exceptional support based on the purpose to halt, deteriorate or pirate the individual verdicts. Hart et al. (2020) considered a national organization's decision-making procedures. Fig. 5 describes the anatomy of a cyber-attack. Based on the USNM approach in regards to the operation of cyberspace, it is observed that network operations are comprised of the security, assaults, and practical utilization, as suggested by Ma et al. (2021)

Alghamdie (2021) has suggested that these operations emphasize data assembling and analysis over the hindrance of the network. Perhaps it would act as a preliminary threat. These operations endorse the distribution of knowledge and purpose, as Thomson (2015) stated. The utilization of computer networks leads to execution operations to snatch essential data. Liu et al. (2021) stated that Doors and Trap sniffers are considered significant types of equipment for cyber particular. Doors are accountable for offering approval to an outside party without computer operators' information. Besides, sniffers are the appliance utilized to snatch passwords and usernames, as Karbasi and Farhadi (2021) stated. Cyberwarfare outcomes are noticed as below stated by Khan et al. (2020), Furnell and Shah (2020), Mehrpooya et al. (2021)

1. Government-authorized system to overturn disasters risk associated with national-level safety
2. Co instantaneousness emergence of physical groundwork and support of physical warfare beginning for the foreseeable future.
3. Disastrous devastation against nations picture at the international level;
4. Catastrophic devastation to the political and economic relations of the nations
5. Expansive individuals' mortalities to maintain public health and security
6. Interior confusions
7. Extensive interruptions in nation governance
8. Deterioration of public reliance on national, theological, and ethnic convictions.
9. Harsh damage to the financial outcome of the nation
10. Expensive deterioration of the performance of national cyber resources

Moreover, five situations could be described in cyber-warfare
(1) Government-advocated cyber espionage in order to assemble data with the assistance of forthcoming device cyber-attacks
(2) A cyber-attack targeted to putting the foundation against turbulence and general revolt.
(3) Cyber-attack targeted at debilitation appliances and assisting aggravated assault.
(4) Cyber-attack as a supplement against physical aggression
(5) Cyber-attacks against enormous catastrophic devastation as the final result of cyber warfare, as stated by Alibasic et al. (2016).

Sun et al. (2018) stated that Cyber-attack utilizes encrypted technology to encrypt and decrypt the information. Encryption can be utilized inclusive of encryption, offering further steps for confidentiality.It could be encrypted and decrypted with the aid of a particular person. Yang et al. (2021) stated that the encryption system deals with encryption and information decryption.Encryption is considered a potent method to assist confidential data while being in jeopardy due to outsider fraudulent and illegal practices from the armed forces.Zou et al. (2020) stated that cryptographic algorithms are found to possess perpetual reinforcement to combat inconsistency due to advancements in computerization. Figure 2 shows the differentiation between cyber warfare, cyber attack and cybercrime.

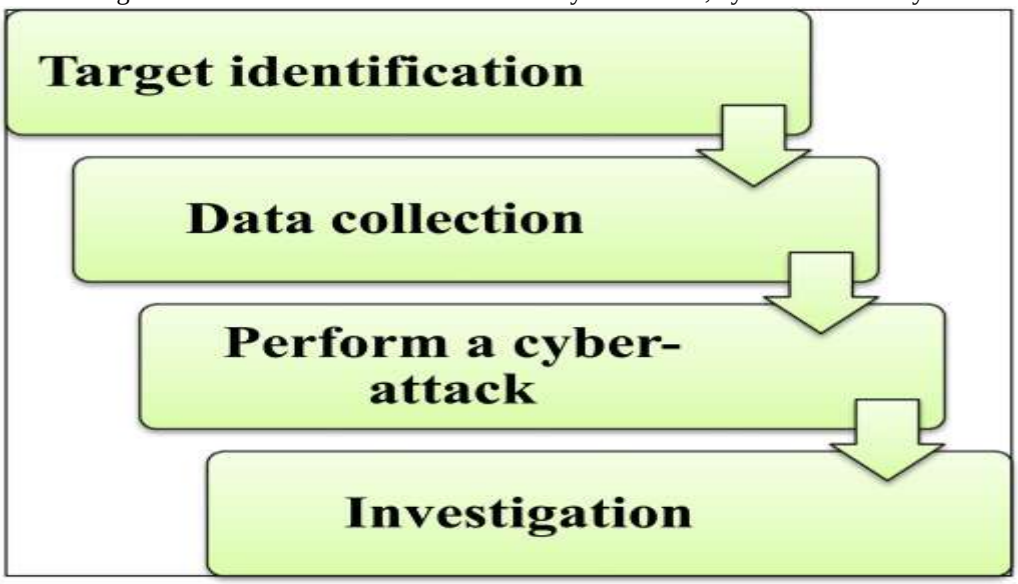

Fig. 5:- Anatomy of a cyber-attack.

Cyberattack Definition based on experts' perspective:
As described below, several definitions are being offered in both legitimate and technical areas.
(1) Richard Clark: Motsch et al. (2020) stated that cyber attacks as operations performed by several nations to penetrate any nation's computer network to trigger impairment or perturbation. Cao et al. (2019) elaborated on the consideration of 3 components: a criminal attack, purpose, and intention behind the assault irrespective of disruption. Moreover, several nations are elaborated context to cyber-attack though, but when non-state and private organizations play in opposition to third states, that lead goes beyond the scope in terms of definition. Therefore, a gap in the legitimate description of assaults is being posed. Zhang (2021) mentioned that the described definition is predominantly insufficient based on the present scenario. Furthermore, it would not be involved assaults conducted by private and government organizations, which results in emptiness.

(2) Michael Hayden: Several studied endeavours to disrupt any nation's computer networking, as stated by Robinson et al. (2015). It is clear from the definition that no differentiation has been observed between cyberattacks, cybercrime, and cyber warfare. It is observed that ambiguity in detection between two lines impacts analysts and policymakers in formulating policies.

The considerable network coupled with rules departs cyberspace that possesses a hazardous and detrimental impact on war propagation and pugnacity context to several nations elaborated by Edgar and Manz (2017). Therefore, in comparison to the first definition, which restricts the criminals' assaults on attackers of government. Nicholson et al. (2012) suggested that this definition, though convenient to express, is shown to have a detrimental impact that creates turbulence between nations and the international community's hazardous threat.

(3) Martin Libicki: Quigley et al. (2015) stated that digital attacks on computer systems cause the attacked computer systems to appear normal but, in fact, produce and issue untrue responses. It has been demonstrated that digital assault on the data processing is responsible for having the computer systems' normal appearance. However, it leads to a deviation in standards. It has been demarcated that strategy to explain the cyber attack precludes many potent concerns affecting nations' safeguard to target cyber structure. Though, attainment in terms of significant assaults has not been obtained.

As a matter of fact, it has been noticed that these assaults pose several threats, including offending the internet system and network of the intended nation. Consequntly, Damon et al. (2014); Shamel et al. (2016). have demonstrated that several cyber-attack definitions do not possess adequate completeness.

(4) Tallinn Manual Group: A cyber-attack is an obnoxious procedure to create a determinantal impact on another individual by property devastation. The perplexing aspect lies in its outcome and impact. In terms of several definition perspectives, a cyber-attack could be considered an assault in case of personal and financial infliction, as stated by Bullock et al. (2021). Thus, this group's prime foundation is based on cyber assaults instead of assaults. From this perspective, attacks that reflect upon effects and violence-associated outcomes, whether impartial or perceptible, could be elaborated as threats. At this step, international legal norms coupled with several areas are implementable, as Chen et al. (2021) stated.

Cyberspace hazardous
Iqbal and Anwar (2020) have reflected on the range of global cyberspace in order to the emergence of superposition locations for regulation of country players possessing several strategies of legitimate and cultural aspects in addition to several approaches to deal with variable strategic interests and several approaches Across the globe; several nations are observed to be contingent upon cyberspace in terms of the tele-transmission and physical world regulation in the sense that shows a certain level of unattainability to cause segregation. Consequently, tasks coupled with the safety and responsibilities of each nation are progressively influenced owing to cyberspace, as suggested by Zhao et al. (2020).

It has become inevitable to offer assurance in terms of provisions of commodities during the supply chain process with the aid of hardware and software product formation at the global level. The cyber area extensibility is associated with variations on a qualitative basis. It is undeniable that bombs should possess a confined substantial range in the abysmal environment. However, cyber-threats lead to comprise a substantial amount of repercussions. So, Real-world scenarios are being regulated with the help of several mechanisms.

Based on various aspects of knowledge, Cyberspace coupled activities are found to be regulated with the help of certain people. It has been observed that operators do not possess the capability to make an alternation in software or hardware. Zhang et al. (2021) stated that it is a well-known fact that few individuals are obliged to have control or management in cyber warfare.The cyber domain dissemination aspect deal with individuals competing against full regulation regardless of appropriate attentiveness and professional competence. It has been noticed that improvisation in cyber occurs at a fast pace contingent upon consistent advancement in communication and computing techniques. In addition to that, cyber cohesion is found to expedite the process. Modification leads to making unprecedented epochs related to susceptibility and feedback. Varg et al. (2021) stated that cyberspace is distant from steady and dynamicism.

In numerous institutions, cyber assets are disseminated in a broader range, starting from tightly regulated government authorized systems to private sector controlled systems in Society. At the time of committing a crime, several assets, capacities, and issues are found, as stated by Zhao et al. (2021). There is no ability associated with the designation of several practices linked with people or institutions at a higher extent of self-assurance. in the context of cyberspace nature.

Al Ghamdi et al. (2021) stated that several dangers involved with cyberspace are described, such as Interior hazardous and supply chain threats in context to several services owning to inadequate ability linked with indigenous pressures.Intelligence activities utilize several pieces of internet-based equipment with the intent to accomplish the collection of intellectual information and practices. At the global level, various cases have been announced with the intent of nations' structures exploitation and devastation which possess internet-based systems, mainframes, and regulators in vital corporations.Beechey et al. (2021) explored a rise in several groups associated with earning currency and assaults among groups. Moreover, in several situations, hackers enter the internet system to articulate things. Based on the existing scenario, the probability of encroaching internet system with a marginal level of education and expertise, uploading adequate programs and contracts by employing the usage of the computer instead of various other websites. In the meantime, the Hacktivism group's political considerations are generally responsible for causing threats against prevalent email hosts and web pages.

On the one hand, Solomon (2017) demonstrated that these groups are responsible for enforcing numerous email hosts by invading websites to notify political information. While on the other hand, some interior discontented with the corporation are accountable for significant cybercrime. These agents do have not a piece of adequate information regarding cyber threats. Since awareness associated with the targeted system avails the endless access for snatching the worthwhile knowledge by hitting the system. Saxena and Gayathri (2021) stated that terrorists act as alternative resources related to the danger associated with devastation, illegal exploitation related to vital structures for restraining the safety of the country, huge loss, the debilitating financial status of the nation, and declining the credibility associated with credibility as stated by Saxena and Gayathri (2021). Cyber threats sources are described in Figure 5.

The cyber-attack strategies considered vital are Logical bombs, Trojan horses, Spam, sniffers, Worms, Abuse tools, service Denial, and viruses. As depicted in Fig. 6, Vital types of cyber types categories are described. In the service Denial strategy, the access of authorized operators related to the system is described. As a matter of fact, from one end, the assaulter is found to immerse the targeted computers with the aid of several messages, and it has resulted in Legitimate data flow. It can cause the prevention of several systems from utilizing the communication of the internet with other internet systems, as suggested by Topping et al. (2021). In the method of the wide range of Denial services, attack occurs from several sources rather than one as it is found to be assaulted by various levels of distributed systems simultaneously. It is conducted with the aid of worms and then its propagation on various computers to assault the target one.

Several Abusive pieces of equipment are found for the public, accountable for recognition and entering susceptibilities in networks with various levels of skill expertise. Moreover, A logic bomb act as the alternative attacker system, which possesses a programmer with the intent to enter code into a program at the time of specific incidents happenings., Therefore, the program is responsible for conducting devasting practices, as stated by Li et al. (2021) and Marefati et al. (2018). Moreover, the sniffer is a program linked to recorded routing knowledge and perspectives for specific data by using the password in which each packet in the data stream is evaluated by Patel et al. (2021).

A trojan horse is responsible for concealing the threat code, and it is similar to the helpful program that operates on the verge of operating stated by Al Shaer et al. (2020). Moreover, a virus leads to tarnishing the system flies linked with the practicable program with the addition of replicating it in files. Infected files are loaded finally in memory to permit the virus to affect other files. Several viruses are required to possess human interference to spreading. While, On the other hand, the worm acts as an automatic program that causes self-transformation by imitating another network system referred to by Aziz and Amtul(2019).

At last, Botnet is a network that acts as a control system to utilize to disseminate malware, spam, coordinated attacks and stealing messages. This system is incorporated into the targeted computer system with the help to permit the illegal operators to use to control the target system at the remote level to attain illegal practices. Kharlamova et al. (2021) stated that electronic soldiers are names given to Botnets.

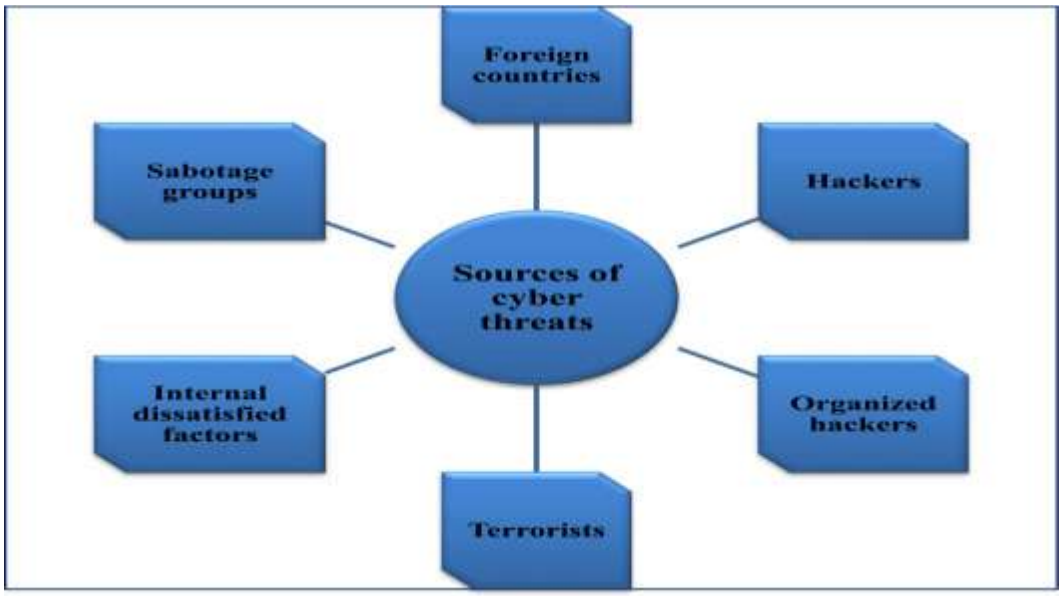

Fig. 5:- Sources of cyber threats.

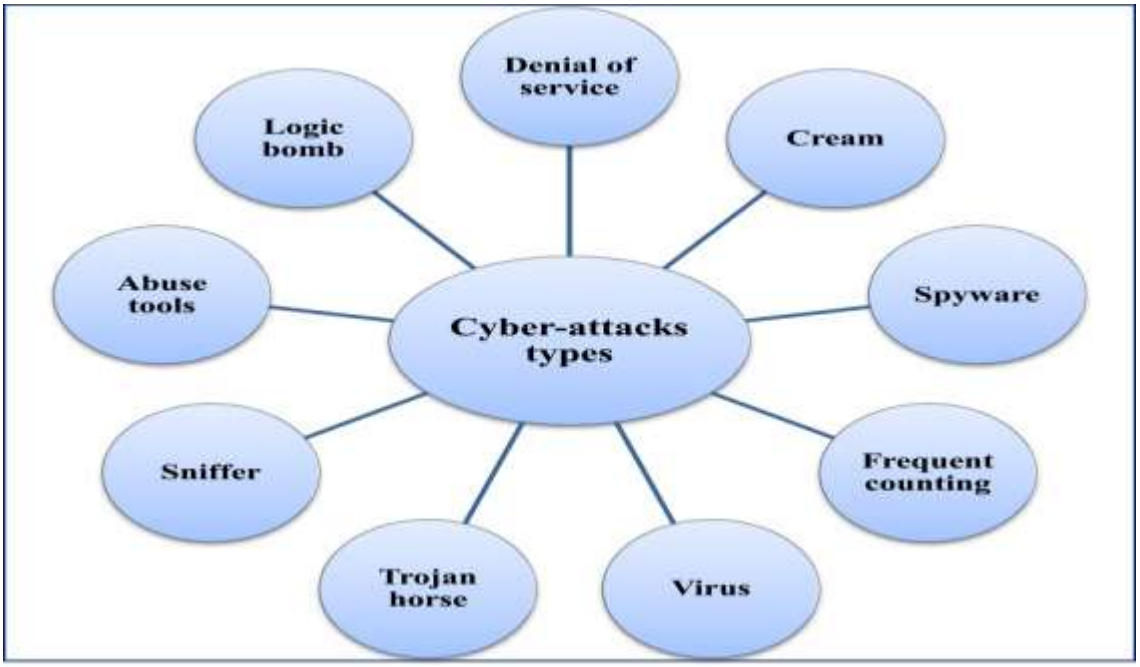

Fig. 6:- Main cyber-attacks types.

Qiu et al.(2021) study has examined the influence and hazards associated with cyber security in WAMS (Wide area management system and control) based FFR (Fractional flow reserve) with new dimensions CNN (convolutional neural network) for handling the stolen information. It has been considered that the cyber security defence structure is linked with fractional flow reserve (FFR). The outcome has demonstrated that synchrophasor data under GPS Spoofing possesses great precision and toughness. Integrated cyber assault procedure based on capital intensive Makrove modelling being created as stated by Lee et al. (2021). Revised HMM uses a security state approximation strategy for the purpose of assessment. With the help of several cases, the effectiveness of methods has been shown.

To counterbalance multistage levels of cyber attacks, a cyber security support system was offered to choose moderate security cases, as stated by Zhang and Malacaria (2021). Both kinds of optimization, such as online and preventive, were utilized in the system for continuous invasions with the aid of LM. Moreover, the Bayesian Stackelberg game for practical resolution is associated with online optimization. Variable to find the probabilities of cyber threat for Net primary production is evaluated as elaborated by Kim et al. (2020). Moreover, AHP and FA were utilized to estimate moderate importance linked with variables of NPP probabilities.

It has been suggested that supreme predilection could be presented as related to the cyber security of Korean strategies. Cyberattacks show an immediate opposed view towards the prevalence of corporations described by Tosun (2021). Moreover, the stock exchange is connected to a company safety violation besides feedback diminishment. Furthermore, the commercial rate is found to be enhanced owing to an increase in marketing burden and liquidity. For a long period, interest and R& D is declined. However, the CEOs are compensated by targeted firms.Progressive digitalization has escalated cyber threats due to the loss of difficult situations to maintain.Eling and Lehmann (2018) stated that it has become vital to recognize the trend of futuristic cyber security and the safety aspects based on analysis. The endurance arises owing to the exposure of devastation threat in functioning process and inaccessibility of several aids poses more threat towards risks associated with a computer-based system.

Causes behind the cyber risk

In the contemporary world, Cyber-attacks are occurring owing to numerous culprits having fragments of cooperative money and the client's economy statement comprised of the banking records and etcetera, as stated by Bryzgalov et al. (2020). The cyberattack occurs as a consequence of offenders who are keen on grabbing clients' or staff members' email addresses in addition to the access details

Current examples

The existing case coupled with cyber risk is malware which is associated with malicious software ransomware virus and worms in operational organizations. In addition, phishing is considered to be the modern instance that the corporate system dealt with, and Russia in cyber-attack comprises the strategy of communication with the help of emails. Therefore, when fraudsters ought to possess the exact password, it has become easier to obtain tremendous data.

Products associated with internet safety

1. Antivirus

Internet safety programs and Antivirus software are capable of designing an apparatus for programming from assault to recognition and mitigating virus. Antivirus software was utilized during the first couple of years when the internet came into existence. However, advancements led to free accessibility to several applications on the internet

2. Managers of passwords

The password manager is considered one of the software applications with the intent to keep storage and management of passwords. Password managers are accountable for the preservation of encrypted passwords, necessitating the people to develop a single master password which could be a strong one that permits the operators to have access to the whole database of passwords

3 Security suits

The security suits comprise firewalls suits, anti-spyware, antivirus, etcetera. This seems to safeguard against stealing, internet surfing private on, security checking of portable storage appliances, and making security associated decisions and are cost-free.

Recommendations:-

Hacioglu and Sevgilioglu (2019) have suggested that it could be advisable to manage the risk assessment business units, and the practices involved are being utilized as a forward-looking practice) with the purpose of comprehending the electronic footprinting of corporations. It would assist in generating a risk register, a document that is employed as a risk management appliance to recognize potent setbacks, as suggested by Hacioglu and Sevgilioglu (2019). A risk management system could be triggered in the process of systemic risk analysis and governance associated with cyber threats with the aid of regular supervision reviewing and upgrading of structure degradation

Literature gap

The research gap consists of the precise data, which was somewhat complicated to assemble by using primary quantitative data of questionnaire forms. On account of the less generation of the questionnaire forms, the exact information in the accomplishment of the exploration had not been implemented yet. There are further obstacles regards to literature gap is associated with timings factors required to make the formulation of the question and gathering in responding to the request

Chapter 3:

Methodology:-

Sample Data Analysis with a questionnaire

Complexity of critical Infrastructure

A critical framework such as energy production and dissemination is increasingly getting more sophisticated, and it is contingent upon the Interlinked device's systems. Over consecutive ten years, electric power systems and other critical frameworks function on an individual basis. It has been observed that these systems are closely related to each other to a certain degree in respect of both Landscape and all segments since the electric network scenario of the United States leads to emphasizing the underperformance level of the critical framework that could bring about a catastrophic impact on the chain of circumstances.

There is no doubt that the susceptibility of the critical framework is associated with the intent to pose a threat to digital life and technological malfunctioning, which has to turn out to be a considerable threat. Furthermore, insecurities are being offered credibility through modern developments. It has been observed that, In December 2015, the world exhibited the foremost power shock, which is attributable to a hostile threat to digitalization. In this scenario, three services of the corporation in Ukraine were affected by BlackEnergy Tryon, withdrawal of hundreds of thousands of residents without no electric energy for a period of six hours.Based on the cyber security corporation Trend Micro, the malware has hit the public-service corporation, SCADA (supervisory control and data acquisition) network, and perhaps commenced with a phishing threat. It has been noted that faint was pursued for two months following reports that show the Israel National Electricity Authority had been subjected to a prime cyber-attack. However, damage impairment alleviated subsequently to Israel Electricity organization terminated the systems to combat the viral infection.

Based on studies, it has been found that finance across the globe is contingent upon the effectiveness of operation coupled with critical framework systems for the existence of Critical framework assets comprised of structures including power delivery, electric circuit, water supply, sanitation, gas conduit, and et cetera. The criticalness of these structures corroborates the dispute for distinct safeguards instead of all kinds of threats. In an attempt to investigate the electronic safety, it has been found that in the space of these crucial structures and various points come into one's consciousness :

- How much Efficiency Level of current security risk evaluation strategies exist in analyzing the potential risk associated with an advanced critical structure system?
- How to make attribution in the interconnection and intricacies of critical framework systems in the evaluation procedure?

Arguably, the modern attack on the computer system against critical framework systems has obliged the requirement for both Investigators and physicians to examine the present evaluation procedures of security related to these structures. Moreover, the frequent attacks coupled with cyber consultants and modern critical framework systems are also becoming intricate due to the combination of modern techniques and massive interrelatedness. These elements are obliged to review the evaluation of security risk dynamics related to crucial structures.

Industrial field subjected to cyber-attack

It has been observed that the power field sector works as one of the prime objectives to deal with cyber-attacks, which were planned against a critical framework. However, it is not the sole sector. In addition to this, Transit systems, the government sector, remote communication, and crucial production companies are also found to be susceptible.

In 2013, an Iranian computer criminal violated the Bowman Avenue Dam in New York and seized control of the stop gates. Oil supply, Boats, artificial satellites, aircraft, airfields, and portal ways are considered to be susceptible, and disseminated information leads to the formulation of several infringements has been gone conducted.

Cyber-attacks against several critical frameworks and prime industrial undertakings have been raised considerably based on the United states cyber-security authorities at ICS-CERT (Industrial Control Systems of Cyber Emergency Response Team). The United States authorities endorse several corporations to assess the threat as opposed to ICS (Indian civil services) and corporation systems.

The panel was informed to have a 20% hike in the digital evaluation for the year 2015 and duplication of threat in opposition to the US crucial production. Throughout the period, a considerable amount of areas have become more credible in the regulation system, which comprises SCADA, Programmable Logic Controllers (PLC), and Distributed Control Systems for the purpose of regulating procedures and regulations of personnel equipment consisting of pumps, valves, motors, sensors, etc.

The Stuxnet computer virus is a noteworthy instance of a threat to digitalization against a critical framework. The worm, accountable for hitting PLCs, obstructed the Iranian nuclear course, which is proven to show a deleterious impact on the centrifuge utilized to isolate fissile components. The circumstances have triggered issues since Stuxnet can accommodate the assault of the SCADA systems utilized through several critical frameworks and building corporations in Europe and the US. It has been observed that in the public instance of a SCADA assault, a German steel factory has experienced massive harm after being subjected to assault on digitalization which enforces the termination of an oven. The German Federal Office reported this for Information Security in the year of 2014. The assailants utilized social engineering techniques with the intent to continue a control linked with the metallurgic furnace.

Research Approaches

Based on the Paquette et al. (2010) study, it has been defined as the word 'risk' is acquired from the Italian word risicare, which leads to the translation in the English language as 'to dare'. NIST SP-30 established a threat concerning an incident's potential implications or consequences on assets or resources and the associated comparable outcome [Paquette et al., (2010). From this side, affirm that threats ought not to be elaborated on or categorized through the magnitude of threats However equilibrating the probable and unanticipated repercussions is recognized as ‘value at risk’ stated by Paquette et al., (2010). It is estimated that statistics evaluation is linked with risk as to the outcome of detriment based on confidence interval probabilities or chances of occurrence. The Obstacles faced by several organizations with references to risk evaluation is when the threat encountered is not evaluated owing to the deficit in the lucidity of evaluation. In this scenario, hazards could be evaluated context to the influence of enterprise based on deficit and expenditure to restore suggested by Paquette et al. (2010)

Cloud computing is applied to a nascent computing model in which devices of massive data processing centres could be applied for offering facilities in a growing manner. Therefore, it has become prevalent in companies in massive scale economical computing. In recent times, the United States authorities have commenced using cloud computing framework, stages, and several benefits to offer services and assist several components. Enclosing the utilization of cloud computing is associated with several harms which could have a vast influence related on knowledge and facilities endorsed with the assistance of technology. A study that has revealed the present utilization of cloud computing authorities and the harm associated with tangible and non-tangible assets and its applications. Analysis of Particular illustration linked with authorized cloud computing, it has been examined that explores the comprehension ability coupled with harms due to several departments and agencies which are accountable for executing this technology. This research has affirmed that specific risk-associated management courses emphasized cloud computing which acts as an integral component of the government IT environment.

This is a role of the use of resources and the expenditure in order to safeguard. The Obstacle is linked precisely to value systems such as ICS-SCADA as operational technologies (OT) that endorse the role of critical framework systems. Confronted with adversity, the organization frequently becomes vulnerable to involve hazardous practices, leading to temporary advantage owing to misinterpretation or inexperience of the put in jeopardy compared to the predicted worth.

Propositions Reviewed

Qualitative features of the concept of threat

It has been observed that the issue of threat has perceived a wide acceptance during recent years and is considerably found to be remarkable across all aspects of industrial and authority level. This is following the subject which has grown to a considerable extent as elaborated by Paquette et al. (2010); Stoneburner et al. (2002); Kaplan and Garrick (1981)

The word "risk" tends to possess several faculties in these published writings. Numerous types of threat risk are mentioned: threats linked to the enterprise, socially vulnerable, financial threats, security threats, financial concerns, war threats, political instability etcetera. Contemporary Key conditions could be coupled to one of the necessities for the comprehensible topics that are found to be consistent and uniform utilization of words. Therefore it ought to be similar to offering commencement on categorizing with the aid of sketching an appropriate meaning among numerous words to make its usage. It could be initiated with risk and Uncertainty.

This project is taken into consideration related to threats that are concerning to the amalgamation of finding what could be manifested, the likelihood of occurrence, and the repercussion of what has happened. This statement is endorsed by Kaplan and Garrick's model stated by Kaplanand Garrick (1981)

It has been found that a quantitative description of the threat is recommended in the context of the notion of a "set of triplets." The interpretation leads to be enlarged with the purpose of comprising vagueness and comprehensiveness, and the utilization of Bayes' theorem is elaborated within this framework. This description could be employed to discourse the ideas of "relative risk," "relativity of risk," and "acceptability of risk.

The differentiation Between threat and vagueness

It has been presumed that an affluent family member who had expired would be nominated as sole heir. The reviewer is adding several resources. Unless it is finished, it has become difficult to a certain level to receive the amount with the help of estate taxes. It could be considered as around $1 million or $2 million. In this scenario, a person can accept the occurrence of precariousness; however, he barely admit that he is going through exposure to hazards. Consequently, the idea of risk comprises unpredictability and the type of impairment or injury that needs to be acquired. Metaphorically, it is possible to record threat in the form of an equation such as; threat = uncertainty +damage. This calculation is described as first class with distinction. As secondary, it is shown to have considerable importance in terms of the distinction between risk and hazard idea that has been described in the following sections to differentiate between the notions of "risk" and "hazard." This is the subject of the next section

The Differentiation Between Risk and Hazard

It has become worthwhile, specifically in the comprehension of widespread arguments concerning the ambient linked generation of power and transportation services for the purpose of extracting a differentiation between the concept of risk and hazard. Based on the dictionary definition, hazard means "a source of danger." Risk is considered the likelihood of "loss or injury" and the "degree of probability of such loss." consequently, hazard, therefore, has occurrence to be emergent as a source. Risk comprises the probability of transformation related to that origin for the authentic supply of damage, determinant, or piece of hurt. It is the essence that deals with the utilization of words. Take an illustration of the ocean, which could be considered a hazard. To make an effort to get through it in a peddle boat raft that experienced a considerable threat. In the case of the utilization of Queen Elizabeth, the marginal risk is associated. Therefore, Queen Elizabeth is considered an appliance for the purpose of safety instead of hazardous things, which led to being associated with minimal probability of risk. Expressing the concept metaphorically employing an equation: described as hazard safeguards risk = This Equation could reveal the idea linked to having probability to make threat so marginal based on interest by expanding the protection limit. However, the threat is never found to reach the limit of zero. It has been noticed that the safeguard word is relevant to the topics that mean genuine consciousness. In other words, risk awareness leads to the reduction of risk. Therefore, if the hole appears around the interjunction of the road is shown to have minimal risk associated factors.

Relativity of Risk

In connection to this concept, it has been investigated that risk corresponds to the spectator. This notion has been well illustrated in the Country of Los Angles. It has been found that few people are found to be accountable for placing a serpent in the letterbox. When people asked about the risk associated with placing a hand in a mailbox, it was noticed to have no risk though the snake is one of the most dangerous species. Therefore, the risk was observed in the context of the observers. It is a personalized approach that relies upon observers. Some authors reference these issues with the help of utilizing a phrase of perceived risk. The concern associated with words indicates the occurrence of another form of associated risk. It is purposed that the presence of "absolute risk." Nevertheless, it was under the influence of pressure to make things clear. Concept coupled with absolute risk is often would eventually be considered as a possible threat. It could be well acquainted with several intense academic questions linked with accidents tending to remind individuals about Einstein's relativity theory. This issue would become lucid after getting the clear-cut elaboration regarding topics such as Risk and Probability. This procedure will be commenced in the following section after defining the meaning of risk. The present decision is related to representation, which isolates a bit from complex arrangments due to the risk term for the probability word. It, as a result, pans out at its best level as the reader additionally possesses appropriate institution abilities for the purpose of comprehending the probability definition. The previous exploration related to the threat would undoubtedly prove to work for the purpose of encouraging the motivation associated with particular consideration offered to the intricacies of probability description. Therefore, on a qualitative basis, the threat relies upon actions, knowledge, and incomplete knowledge progression in new concept would be quantitatively based.

Quantitative definition of risk (first level)

For the assessment of risk, it has become easier to put effort into anticipating the future in case commitment associated with specific action occurs. Therefore, it is obvious to have a risk analysis approach that entails the answers to subsequent questions :

The set of triples is observed for QRA (quantitative risk assessment) based on the model. According to their model, quantitative risk assessment (QRA) is based on 'the set of triplets':

✓ What can happen? ✓ How likely is that to happen? ✓ What will be the consequences if it happens?

It refers to the Kaplan's first risk function based on the likelihood associated with undesirable outcomes and intensity related to repercussions of particular incidents stated by Kaplanand Garrick (1981)

This leads to Kaplan’s first risk function as the probability of an unwanted event and the severity of the consequences of such an event described by Kaplan and Garrick. (1981):

$R = \{<Ti, Li, Ii>\}$ (1)

Where Ti represents the risk scenario; Li describes the probability of this particular situation, and Ii denotes the resulting impact.

The situation is highly indispensable to the risk definition suggested by several projects. By prolonging the consideration, it has been observed that Kaplan's definition of risk is linked with the likelihood of the system migrating from one nation to another one according to the t (function of time) and c (completeness) stated by Kaplan and Garrick (1981)

Following is the state of risk R equation described below :

given the new state of risk ‘R’ as

$R = \{<Ti, Li, Ii>\}c$ (2)

Kaplan's model is altered to include the probability of incidents occurrence and its potent influences. Nevertheless, is fundamental existence on which influence could be quickly evaluated upon which impact can be assessed. It could be termed as an asset 'A'. In addition, the concern is considered to be insignificant owing to the lack of susceptibilities. Threat 'T' is therefore presented as an activity of susceptibilities. It has led to the alternation in Eq 2, which leads to (Eq 3) Equation (2) above, leading to Equation (3):

$R = \{< V (Ti), Li, A(Ii) > \}c$ (3)

The introduction of asset 'A' and vulnerability 'V' in (3) leads to accomplishing worthwhileness in broad level elaboration coupled with system risk. Based on Eq 3, a novel model is elaborated, which could be considered as a

function of P (probability) of T (Threat) events employing the V (Vulnerability) and its severeness that is assessed as the result influence (I) on A (asset)) From Equation (3), a new risk model is defined; as a function of probability (P) of threat (T) events exploiting the vulnerability (V) and its severity, measured as its outcome, impact (I) on an asset (A). (Therefore, risk evaluation is defined in Eq 4 with the following vectors: (asset (A), threat (T), vulnerability (V), likelihood (L), and impact (I)).

$R = \{< ((V (Ti,) Li, A (Ii))t>\}c$ (4)

Based on Equation (4), It can be derived the prime factor coupled with novel risk evaluation models see fig 7, and it has been suggested that dynamic modelling in order to evaluate the safety threat associated with critical framework structures.

Structuration of Approaches

The following structures are described as the project structures :

In Section 2, state of the art coupled with the security risk of critical infrastructure systems. Then research methodologies will be described in Section 3. . In Section 4, the data analysis and results, and the discussion will be elaborated. Then, the conclusion will be discussed in Section 5.

Chapter 4:

Data Analysis and Results Discussions:-

Associated Researches

Critical framework systems

The critical framework is described extensively on a massive level to illustrate the social and technical system, which offers several facilities to the community and is indispensable for adequate operations, as stated by Bruijne and Van Eeten (2007). There is no doubt that a critical framework performs a considerable Importance in terms of social amenities and social life. It has been observed that the several interpretations of categorization in terms of necessary framework.

It has been noticed that several other procedures consist of measurement of gas handling and conveyance alongside the regulation of storage and security check. The tremendous requirement for perceptibility from manufacturing facilities and striving forward the process of refining competencies and the eagerness to curtail the business expenses being utilized by retail investors and management personnel leads to enhances the automatic regulation in the energy field endorsed by the development in electronic industrial control systems (ICS) and logic-based digital systems. It has been noted that DCS (Distributed control systems), HMI (Human-machine interface), PLC (Programmable Logic controller), VFD (Variable frequency devices) and SCADA (Supervisory control and data acquisition), and SIS (Safety instrumentation system.

In conjunction with general Information Technology (IT) systems that offer an endorsement in company knowledge and data processing, the control systems appliance or equipment function as the operations technologies (OT), after that critical framework systems function. Based on the inclination toward enterprise leaders, business owners are confronted with the management of two assemblies.

IT system for enterprise knowledge and Operational technologies (OT) for operations.

In contemporary times, this merging might not be considered a general one; however, widespread and enterprise lead implies an appropriate OT information maintains the communication with IT system as per suggested by Bodungen et al. (2016).

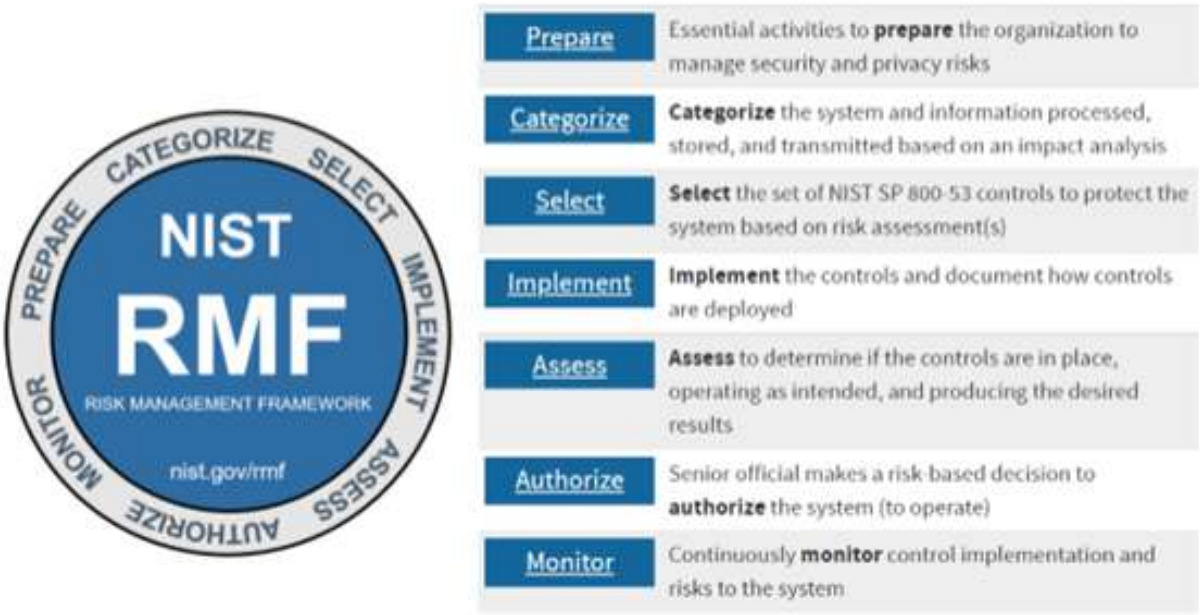

Figure 7:- NIST Risk Management Framework.

As shown in Figure 7, The NIST Risk Management Framework (RMF) states that extensiveness, pliability, reoccurrence, and the measurable 7-step procedure which any the corporation could utilize for the management of information safeguard and confidentiality threat coupled with corporation systems are connected with a set of NIST criteria and regulation to sustain the execution of risk associated management course to satisfy the need of the Federal Information Security Modernization Act (FISMA).

Based on the structure, the subsequent steps would be followed:
- Systems Characterization - Threats Identification - Vulnerability Identification - Control Analysis - Impact Assessment - Likelihood Determination - Risk Determination

Risk evaluation in Critical framework structure
It is undoubtedly true that advanced levels of associated industrial procedures threaten the industrial control space. It has been established that logic-based digital appliances are found to be vulnerable to several probable collapses that do not generally exist in the hard-wired analogue structures, provided that several programs procedure like ControlNet, DeviceNet, Profibus, and Serial Modbus were contingent upon protocol, vendor-specific techniques as per suggested by Bodungenet et al.,(2016). It also indicated a thrust to make utilization of advanced techniques like Linux, Windows OS, and Ethernet protocols (IPs) to regulate, check and display controlled actions. This confluence has brought about a novel kind of safeguard threats that were unfamiliar prior to the year 1990. The conventional indirectly leads to the theory of the safeguard related to critical assets, which follows the concept of restriction to cause physical constrain around resources, elements, or boundaries which requires safeguard as stated by Pieters (2011). This is in cognizance of 'inside' opposed to the 'outside' is debatable in the interlinked ambient since it becomes tedious to distinguish between insiders and outsiders linked explicitly to the critical framework platform

Research Analysis
Contemporary critical structure assets based on several features and formulations have become reliant and significantly correlated with enhancing structure intricacies. In such space, it is not used to be lucid in which corporation demarcation has made it tedious to execute the conventional perimeter system. Security threats are correlated with critical framework procedure has presented extensive amount of physical, logical and technology impairments established infrastructure system and ambience. . At that spot, it has been observed that several resources of fear could be displayed.

It has comprised of individual failure, technological error, technological annihilation, qualified offerings, departure of standard offerings, standard services, application/protocol threat, Intentional action of vandalization, premeditated action of digital knowledge exploitation, DDoS, Botnets, web interface attack, and advanced persistent or state-sponsored threats [Wei et al.,(2004); Dahbur et al., (2011); Johansson et al., (2011)]. There are other specific areas of hazards which consist of Water Hole attacks, Ransomware, Dropper, Rootkits, Spyware, Worms, Trojan Horses, Phishing, and Spear Phishing.

Institutional threat Evaluation Standards

During the past few years, several evaluation models associated with risk have been suggested to demonstrate the safety threat evaluation notion which could be demonstrated. Following are the six models which are being elaborated on.

NIST Evaluation of structure (SP800-30/30rev1)

NIST2 elaborates threat evaluation as the fundamental category of corporation - more significant threat linked management procedures, as elaborated in NIST SP 800-39. It has been asserted that the significant role of knowledge associated with security evaluation is linked with recognization, evaluation, and giving precedence to corporate business such as aim, operations, images, and prestige. From the presentation date, interconnection exists between corporate resources and individuals with the assistance of information resources. It has been observed that intention linked with operations, corporations assaults, susceptibilities, and influences ought to be assessed for the recognization of essential patterns and decisions to be cognizant regarding the direction of putting efforts to eradicate or decline concerns of threat capacities, declining susceptibilities and making the evaluation, coordination for cyberspace workings. This is intended to elaborate on the decision-makers and endorse risk assessment with the aid of recognition.

➢ threats to organizations and against other organizations; ➢ vulnerabilities against both internal and external organizations; ➢ impact to organizations that may occur given the potential for threats exploiting vulnerabilities, and the likelihood of the threats occurring. The result of the assessment process described in Figure 7

4.2.1.2 ISO/IEC 27 005:2008

ISO/IEC 27 005:2008 examine risk evaluation procedures in regards to organization-wide risk management practices and recognizing the prime evaluation procedures, a threat recognition analysis, and evaluation as described in Figure 8:

SO/IEC (the International Organization for Standardization and the International Electrotechnical Commission) is part of the specialized systems for worldwide standardization.

4.2.1.3 Focal point

Threat recognization:

The approach of exploration. Recognization and data compilation related to threat elements. It engenders in the recognization of sources such as hazardous in regards to body sufferings, incidents, circumstances, and scenarios linked to possessing considerable influence on system aims and the extent to have probabilistic influences, e.g. hazard in the context of physical harm, events, situations, or circumstances which could have a material impact on system's objectives and the nature of the possible impact. This study is being targeted to recognize the occurrence of possibilities associated with specific scenarios leading to influence performance coupled with the targets of the system. The aim is to identify what might happen or what situations might exist that could affect the achievement of the system's objectives.

Risk analysis:

It consists of constructing deep alertness related to the challenges of the system. It offers entry to the evaluation of threats, contingent upon threat ought to be addressed and specific layouts, approaches need to be embraced. It inputs risk assessment decisions, whether risks need to be treated, and the appropriate schemes and methods to be adopted.

Risk assessment:

it utilizes the comprehension of threats acquired at the level of analysis in order to conclude in regards to prospective operations. The main aim for the evaluation of the worthiness related to stags of risk and then make the comparison of predicted safety threats with established threats

The purpose is to determine the significance of the level systems' risk and compare the estimated security risks with the criteria defined by the established context. ➢ Risk decision: It offers entry related to threat decisions regarding forthcoming practices. Several other entries need to be included while taking decisions, such as ethics, legitimate, economics, and several other things belonging to the understanding of the threat. Following standards need to include while the decision is taken. The decision-making criteria include: ✓To know threat requires to be addressed ✓ preferences for addressing the issues ✓ practices need to be considered, and ✓ Paths number is required to pursue.

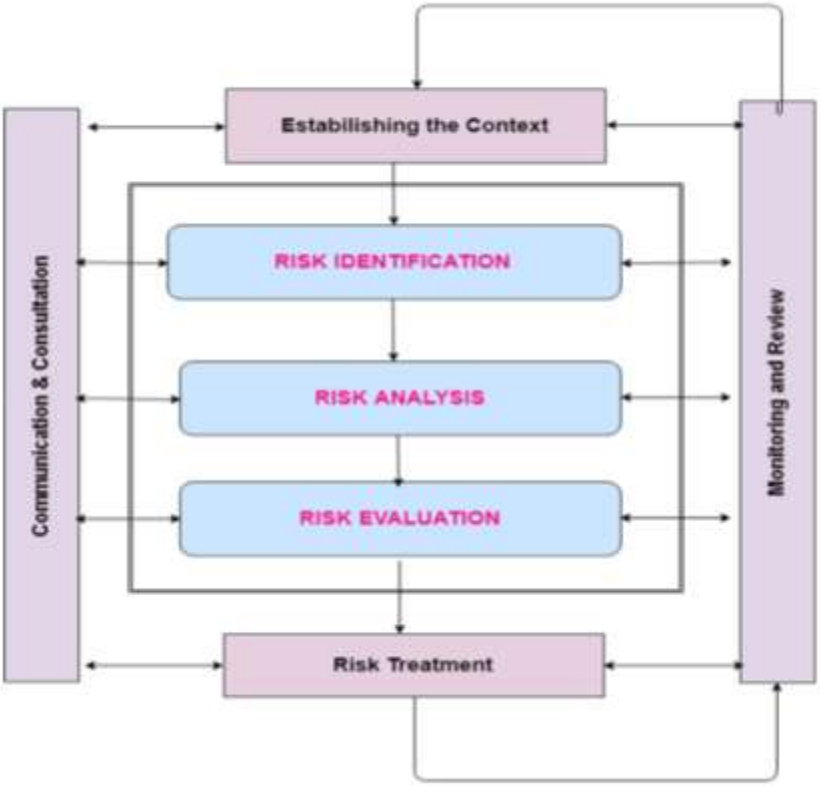

Figure 8:- ISO / IEC Risk Assessment Framework.

Investigation equipment

The BS-7799-2006 encourages the involvement related to procedures strategy to evaluate, address, regulate, and notice threat exposure, as stated in Figure 9. The aim ought to be coupled with the promotion of guardians for the purpose to pinpoint on the significance

✓ Comprehending enterprise-related knowledge regarding safety standards and requirements to make policies for elucidating the knowledge of safety targets. ✓ Selection, execution, and operation regulation in terms of corporate management related to enterprise exposure of threat✓ Checking and regulation of achievement and effectivity for Information safety management system and, ✓ Incessant assessment of current safety threat measurement operations

Figure 9:- BS-7799-2006 risk assessment framework.

Business Models

In this scenario, three models of business-wide evaluation would be considered for accommodating how these procedures could vary from organization categories as described the above

Octave

The octave model is an enterprise-wide risk evaluation model that is employed in the measurement of information technology exposure to threats in terms of business workings and strategic operators. It is not similar to the priorly elaborated models of OCTAVE as a qualitative standard that leads to aiming the assessment of corporation business threat endurance stages, as shown in Figure 10.

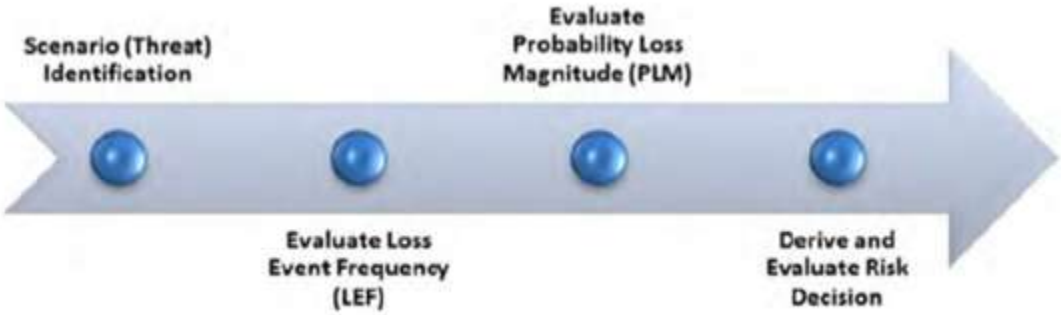

Figure 10:- FAIR security risk Assessment Framework.

Microsoft

Microsoft information safety threat management comprises four procedures, as shown in Diagram 11

❖ Assessing risk ❖ Conducting decision support ❖ Implementing Controls ❖ Measuring program effectiveness

Elaboration of the typical risk evaluation structure

Lacuna in the current structure

In contemporary times, academics, physicians, and safety experts, on the whole, have been handicapped by numerous obstacles, not to the minimal level, which is incompatible with its nomenclature. In a specific framework, software shortcomings are mentioned as 'threats', concerning implications coupled with similar flaws are specified as a 'risk', and still, others pertain it as 'vulnerabilities'. In addition, the resulting turmoil is incompatible, which is the supplement troublesome in delineating and standardizing safety risk evaluation. It is not expected that organizations, businesses, and academics are being ineffective to some extent to consent to the general strategy to evaluate information safety risk, as shown in Table 1

Moreover, the Junction between critical frameworks and their linkage is not effectively investigated by actually existing research in the point of view of cybersecurity threat evaluation as described in Table 1 Summary of Common risk assessment frameworks, insignificant degree of revised structure has an emphasis on critical framework systems such as controlled systems. Furthermore, in writings that include some research being conducted which have been constrained for the intention of recognition linked with the risk measurement assessment as shown in table1.

It has been described the holistic procedures during the exploration of the investigation. Indeed, as illustrated in the writings, the concerns of recognition strategy contradict the evaluation procedures that encompass structure progress and safety policy assessment, as observed in the research. Remarkably resources portray an assessment that this research might include as a fundamental feature of safety risk evaluation in critical framework procedures not addressed effectively in the present structure. Contemporary corporates rely upon critical structure assets, considered one supplementary component of organization assets. These assets are crucial for enterprise viability in terms of expenditure and values.

Consequently, The threat evaluation ought to recognize and value the critical framework system. Afterwards, the influence of risk would be assessed. Moreover, quantitative evaluation without resources assessments is considered an additional concern for assessors and probably more concern for the mutual dependent crucial framework.

The obstacles to estimating the codependent critical structure to construct the utilization of dynamic simulation in evaluating risk-coupled procedures were found to be highly preferable. In addition, existing research based on the concept mentioned earlier discloses the discrepancies and inadequacy of agreement among the organization and corporates such as BS7799-2006, OCTAVE, NIST SP80030, BS7799-2006, ISO/IEC 27 005-2008, OCTAVE, FAIR, and Microsoft. The cause behind the discrepancies among evaluation procedures leads the situation to further exploration.

Figure 11:- Microsoft risk assessment framework.

Dynamic Modeling Of evaluation procedures Process

It has been acknowledged that the risk evaluation model follows systems dynamics. The level of evaluation procedures considers the risk measurements as described in Equation (4), which is found to make the foundation of the suggested model. From Equation 1.4, basic supplementary structures are presented: threat/vulnerability pair (TVP), control assessment (CA), risk modelling, and risk policy evaluation, as described in figure 12 of the security risk assessment framework. The association and disparities between the suggested and current models are shown in Table 1 of the Summary of the common risk assessment framework.

Institution	Publication (number)	Description	Focus
NIST	SP 800-30	Risk management	Information systems (General IT systems)
NIST	SP 800-37	Risk assessment	Information systems (Federal information system
NIST	SP 800-161	Risk management	Supply chain management
ISO/IEC	27005	Risk management	Information systems
ISO/IEC	31010	Risk management	IT governance
ISO/IEC	31000	Risk management	Organization wide (general)
British Standard	100-3	Risk analysis based on IT infrastructure	Information technology
CERT	**OCTAVE**	Operationally critical threat, asset and vulnerability evaluation	Enterprise (IT) projects
FAIR	FARE	Risk identification	Business information systems
MICROSOFT	MICROSOFT	Risks in the perspective with data acquisition and storage	Software and data
MODELLING		**Risk assessment in complex (interdependent systems)**	**Critical (complex) infrastructures**

Table 1:- Summary of the standard risk assessment framework.

System depiction

The issue in the case arises from the question: what is the environment to be assessed? In monitored conditions, critical assets comprise knowledge and service techniques such as software, hardware, database, procedures, individuals, and networkings that lead to endorsing the enterprise's knowledge and workings procedures. As an alternative, the emphasis is coupled with resources that endorse subsequences procedures concerning particular pinpoints on regulated advancements.

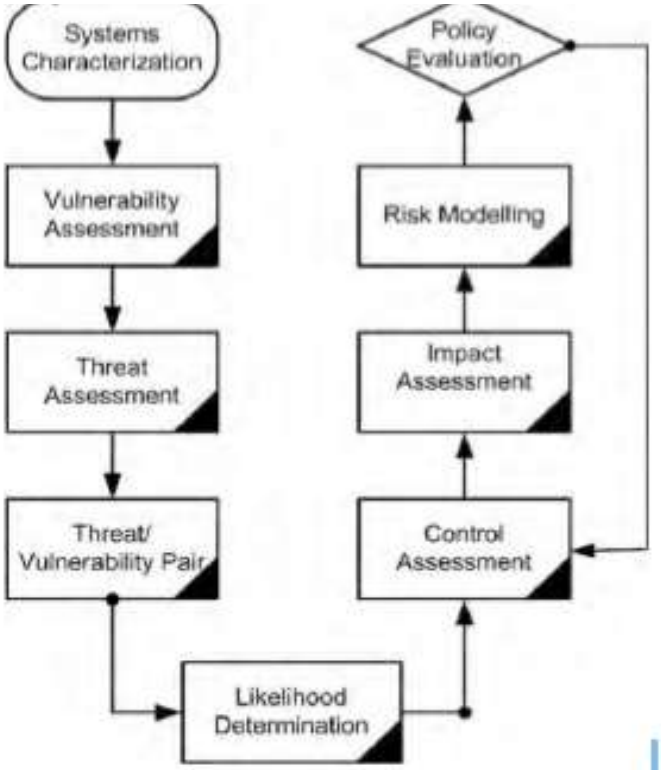

Figure 12:- Security risk assessment framework.

Resources recognitions

One question comes under this category: What is the IT framework and crucially advocated enterprise workings? It has been observed that the specific target coupled with risk evaluation in this instance is to recognize and delineate

the critical resources for safeguard, evaluation, vessels, and guardian. In the power field, the emphasis is given to the resources that aid in downstream workings after specific consideration of regulated advancements.

Threat investigation

What is the systems' threat vulnerable? It described certain circumstances of operation and inactivity context to specific actions and inactions suitable for exploiting the system's susceptibility. It could be observed that players whose incidents could breach the system safeguard with adverse repercussions. Another study has revealed that recognition of subsequent threat origins for the viability of any critical systems stated by Touhill and Touhill (2014)

✓ APT (advanced persistent threat) Sawyer and Jarrahi (2014) stated that: ✓ Intentional actions of secret services or violation ✓ Hacktivists ✓ Service inclination from delivering services ✓Intention action of destroying or malicious mischief

✓ Technology obsoleteness ✓ , internal pressures, and ✓ Low-quality products and offerings

In addition, resources comprise unforeseen circumstances such as deluge, hurricanes and tornadoes, etcetera, environmental concerns including flame, electrical power failure and anthropogenic elements such as inadequate data entry and illegitimate accessibility, software engendered fear consist of phishing, bots, malware, and SQL injection etcetera

Suceptiblity Evaluation

It could analyze the feebleness coupled with the environment would be harnessed through fear actions. Susceptibility is considered the system's average vulnerability for assault owing to adverse incidents, as Johansson (2010) stated. In a regulated scenario, susceptibilities of the system could be categorized from two viewpoints, such as a global perspective in which overall susceptibility associated with the system due to expiration of threat would be observed. Another viewpoint would be linked to the evaluation of critical elements to which the system is found to be susceptible stated by Apostolakis, and Lemon (2005)

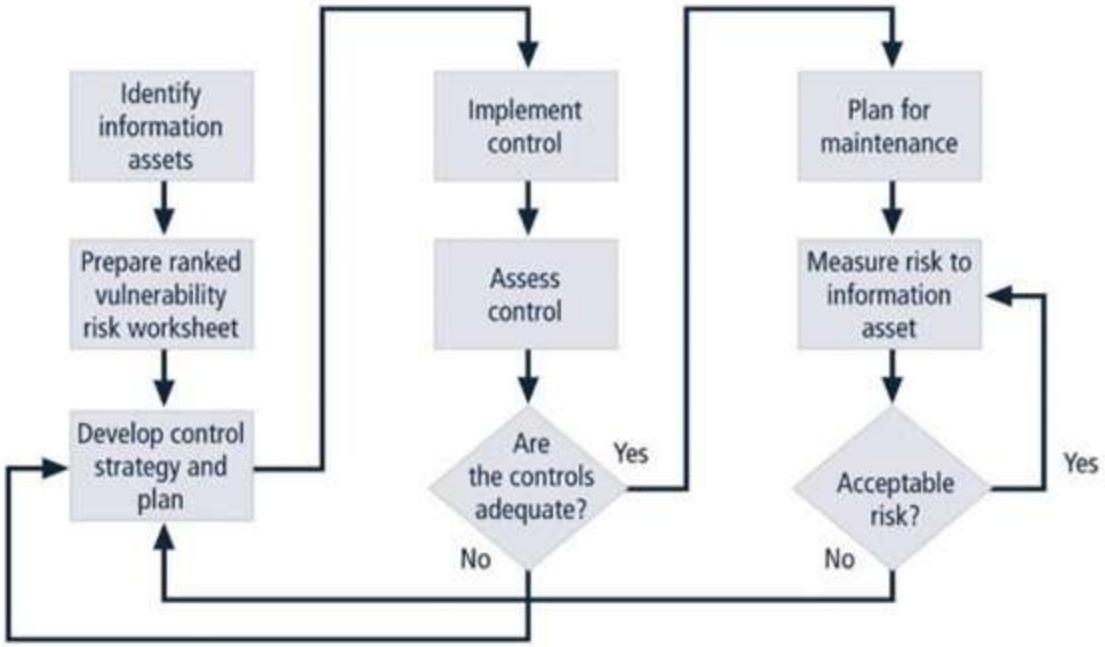

Figure 13 Security risk control cycle.

Hazard

Vulnerability Pair TVP is presented as the coordination between fear and several susceptibilities. It includes complementation of hazardous player to susceptibility. It has been suggested that the subsequent TVP in a TVE (threat vulnerability event) rating, as shown in Table 1 . This act as a quantitative evaluation for the suggested assessment: 0.1 (as very unlikely) and 1.0 (as most very likely)

Analysis of Control

What remedies are in position for systems' safeguard? The mission targeted is associated with evaluating existing remedies accountable for resource safeguard instead of probabilistic threat players, as described in Figure 13. In simulation practices, it is demonstrated that the presence of efficient remedies declines the success rate of threat players at a considerable rate to influence the system's susceptibility, as described in Figure 20. It has been suggested that the subsequent control related to the effectiveness index is described in Figure 14, which acts as quantitative evaluation ways for measurement of the assessment process, as shown in Figure 15.

Likelihood determination: This is a quantitative evaluation of the probability of the threat vector harnessing the TVP (system vulnerabilities) system's vulnerabilities (TVP), evaluated as a function of existing remedies defined in 7.
Lt=[(V(A)□ T)/C)]

Likelihood values are scaled from 1 (very low) to 10 (most likely). Where Lt is the probability of an assault at a particular time interval of t, V is system vulnerability as a function of the asset ('A'), and C is the available security controls (SCs). The divisor (C) feebleness probability of the Attack. It has been seen that the more the value, the decline the probability of threat exploitation and vice versa, as shown in Figure 15

Risk scale	Events counts	Risk score
Very likely	>100/year	1.0
Likely	≥50 < 100/year	0.8
Somehow likely	≥10 < 50/year	0.6
Not likely	≥1 < 10/year	0.4
No Chance	<1	0.1

Figure 14:- TVE Score.

Analysis of Impact

It has been investigated that the influence of threat penalty on the crucial system and enterprises workings. Its main target is to evaluate the range and severity level due to failure of the sources depending upon threat vector attainment. Therefore, the influence in context to loss and expenditure would be measured. The severity of the loss is found to correspond to the resources settlement. One of the studies has been accompanied by the influence of threat assaults with the aid of ALE (annual loss expectancy) by loss in probabilities, as described in Silver and Miller (2002).

Systems Dynamic Modeling

It has been showcased from the above measurements a dynamic modelling strategy as a substitute to current risk evaluation procedures. As shown in Figure 14, the procedures basics of the modelling development pursue a paper represented by Sterman (2002.) 'System Dynamics: Systems Thinking and Modelling for a Complex World' and from his work System Dynamics Modelling stated by Forrester, (2003). Two types of reflection were described such as ✓ structural analysis and ✓ dataset analysis. The structural analysis comprises an exploration of the model framework related to the system underneath particular considerations. However, it involves the exploration of system variables datasets to analyze the conduct of Systems dynamic needs exploration of intricacies engendered through codependencies of systems and associated safety threats extended through system inherited susceptibilities. The strategy offers the comprehension of normal structure and basic intricacies of codependent structures. Based on Riniali, it has been observed that the sheer complexity, magnitude, and scope of critical infrastructure systems make modelling and simulation important elements of any analytic effort.'

An investigation has been explored that modelling and simulation act as pivotal elements for safeguarding, credibility, and viability context to the operation of critical frameworks [Rinaldi et al., (2001)]. This is described as a strategy to include depth analysis of scenario intricacies and policy resistance stated by Sterman (2002).

Sterman's argument endorses the proposal that dynamic modelling offers a systematic strategy to tackle the intricated systems.

Dynamic Hypothesis

This hypothesis aims to engender the risk security evaluation linked to the critical infrastructure systems. There is a subsequent hypothesis described as ✓ Infrastructure codependencies accelerate systems intricacies which a resulting rise in the probability of systems security threat exposure. ✓ The system's susceptibility level correlates to the probability of a threat attack. ✓ Insufficient SCs raise the probabilities of threat assault to increase the influence.

Test 1	High threat level		Low vulnerability level				Weak SCs		
	0.9		0.1				0.4		
Test 2	High threat level		High vulnerabilities				Weak SCs		
	0.9		0.8				0.4		
Test 3	High threat level		High vulnerabilities				Strong SCs		
	0.9		0.8				3.4		
Test 4	High threat level		Low vulnerability level				Strong SCs		
	0.9		0.1				3.4		
Test5	Test 2 + low asset value	Asset1	Asset2	Asset3	Asset4	Asset5	Asset6	Asset7	Asset8
		100	100	100	100	100	100	100	640
Test6	Test 2 + high asset value	Asset1	Asset2	Asset3	Asset4	Asset5	Asset6	Asset7	Asset8
		7065	780	12430	1806	2018	11050	3957	4730

Figure 15:- Simulation (Likelihood of Attack) user-defined parameters.

Modelling of structural codependencies

It has been described that the dynamic model for infrastructure codependencies acts as a completed system to evaluate the pattern of behaviour related to the system and subsystems. As shown in Figure 15, the interplay between elements of the system occurs to engender the behaviour pattern with the help of user-defined measurements. The incidences sequence endorsed in the investigation of the foundation of system safety risk exposure helps probe the basis of systems security risk exposure.

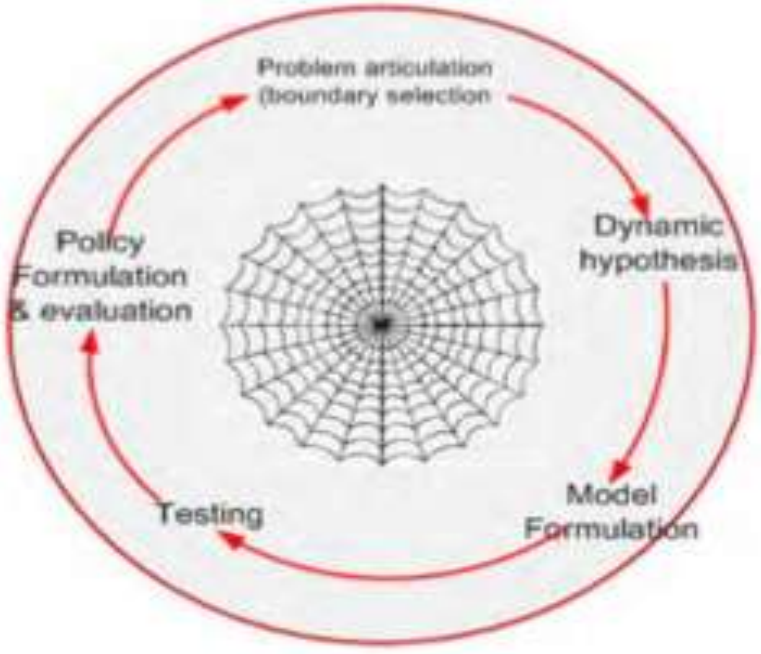

Figure 16:- Dynamic Modelling Process.

Codependecies causal loop diagram

A causal loop diagram elaborate structures of prime variables emphasizing several elements influencing the structural outcome and creates attitudinal variations

Prime implications:

Causal loop diagram in technologies consolidation as shown in Figure 15. This elaborates the strength and probabilities that form the system conduct. As the model at this level has not been executed, however, the Vast majority of descriptions are following supposition inferred from cooperation with framework drivers, executives, and governs who are being classified as the SMEs (subject matter experts). It has been described the several probabilities are: ✓ Technology consolidation applies to the incorporation of the ICS-SCADA infrastructure structure and the technical support. The combination cause codependency related to structures. ✓ Technology integration hazards ✓ Technological assigning people for risk. It has been presumed that more the SCs rate leads to a decline in the average risk of deployment. In addition, higher or lower exposure to risk is supposed to influence technological consolidation. It is acknowledged through loop feedback influence of B3 likelihood maintenance.

✓ System evaluation. ✓ Technology integration performance is a post-acquisition outcome measurement process linked with reinforcement or balance. The indicator follows three prime indicators: ➢ the system's expected performance ➢ and observed ➢ actual performance.

✓ R3—system evaluation findings: Alteration in system practices was measured due to the consolidation of technology. To avoid the measurement coupled with a comparison of structural behaviour observation with its practical outcome. The lacuna is associated with engendering additional evaluation rates due to influencing the consolidation. The feedback twist represents a reasonable force expressed by R1. ✓ B3—technology integration influence: structure competencies influence the structural outcome. In Chapter 5, it has been showcased that the Bedell model reflects that technological consolidation influences structural outcomes. The disputation is extensive to comprise the influence owing to the technical risk associated with deployment. ✓ B3—integration performance index: Technological consolidation could give rise to advancement in structural outcomes. An appropriate degree would bring about a decline in structure resources that leads to feedback return to influence the outcome of structure. It is illustrated through the balancing loop of B3. ✓ R3—integration benefit index: It has been presumed that technological consolidation influences system outcome in addition to the structural finances system.

Enhancement regarding the extent associated with finance is found to be predicted with the intent to bring out to ameliorate structural outcomes. As the model is manifested beyond the mathematics basis, the conduct associated with supplies and surges could be illustrated by engendering at an intermittent interval groove with the help of various databases linked with stocks and flows. Under these circumstances, models are accomplished with algebraic terminology and suppositions that denote the interaction of changes in the model.

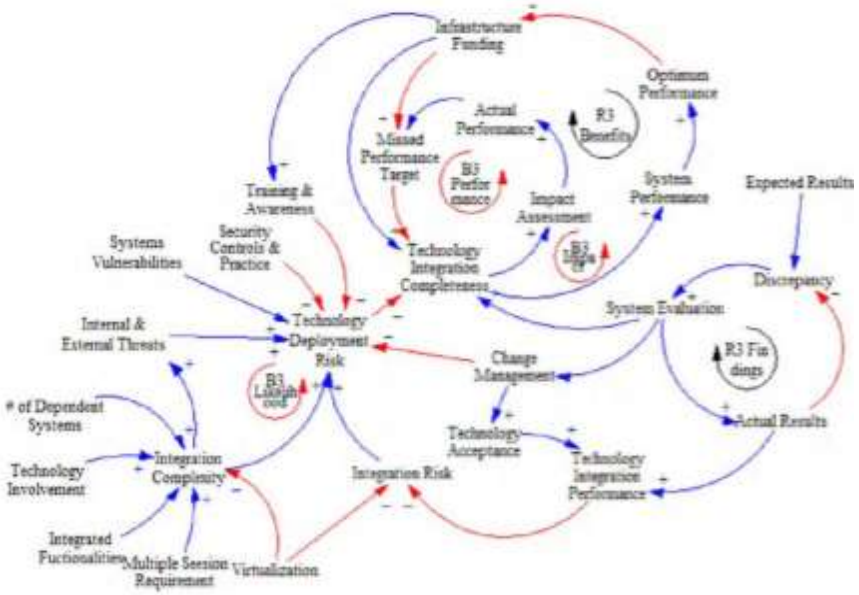

Figure 17:- Technology Integration causal loop diagram.

Simulations and Examinations

In order to determine the behaviour of the model, a stock and flow picture related to chief measurement is represented. ➢ The likelihood of Attack is shown in Figure 12 of the Dynamic modelling process stated by Sterman (2002). and ➢ Impact of Attack in context to effects of system's breakdown in the Figure 17 diagram.

Likelihood of Attack with or without remedies

Figure 1 6 denotes the Dynamic modelling process, which illustrates a snapshot of attack simulation associated probability. The slider permits the operators to handle the actions of the variable at certain data sets with the help of assigned values. Pointers are intended to be effective decision-making types of equipment to regulate the simulator's entry. It has been observed that models alongside sliders such as alteration in management, multiple session need, etcetera are observed as steady in which leading outcome indicators related to simulating variables are described. Constants are datasets that are established before the beginning of the simulation. Besides, attack likelihood rate is linked with flow depicting a constant movement of a determined amount with time. It has been seen those rectangular box variables (stocks) which reflect upon the storage capacity of a certain level that could be preserved or withdrawn with time. Moreover, arrows between variables show the connection between different variables. Sliding motions change the values of the fundamental variable. By taking into consideration that slipping towards the left side of system susceptibility decline the extent of susceptibilities of the system.

Security controls

The exact complete active control rates determine the SC rate. The frequency of occurrence related to active controls splits the rate of probability of assault that depicts the probability of the system related to posing towards danger. In this scenario, the probability of threat assault could be declined with the rise in active System control. The simulation is followed by maintaining the equivalent slider, whether associated with a decline or increase in fundamental measurement rate System control variables could be evaluated based on the scale of 0.1 (very weak) to 1.0 (highly strong). This evaluation is worthwhile for analyzing digitally and also for operational reasons according to the findings of SMEs, as shown in Figure 18

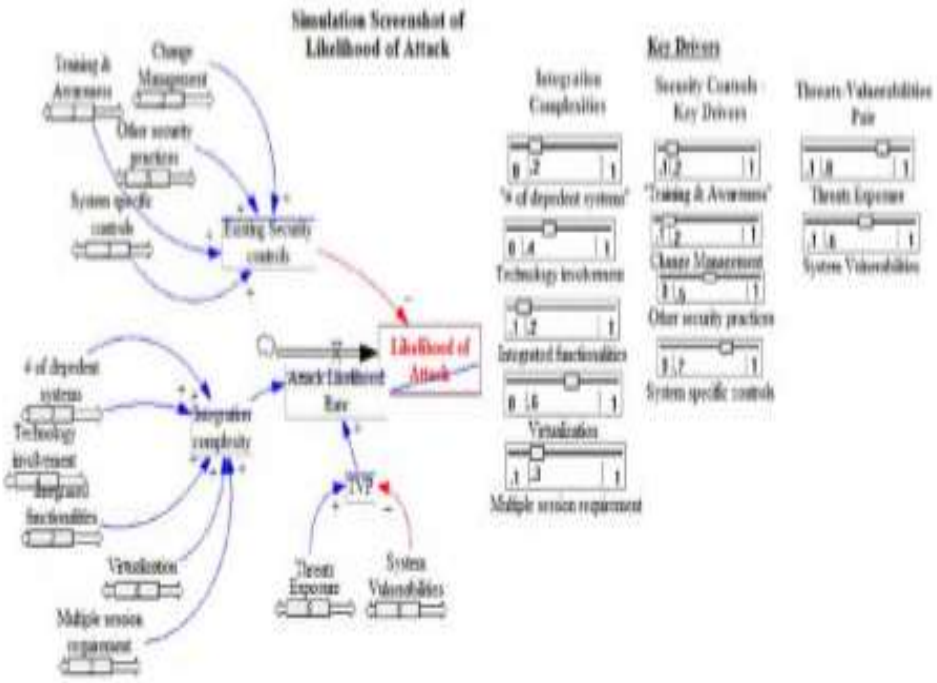

Figure 18:- Likelihood of Attack (without control).

Enterprise influences on safety practices

After evaluation of the influence related to Attack is simulated with the aid of average expenditure of the systems described as cost of assets + total Revenue to be produced. The resources expenditure is predicted, comprising constructive expenditure, the cost associated with maintenance, restoration of cost, and legitimate and regulatory

compliance such as expenditure of legal scenarios. Income comprises Revenue which contains system amassment from the outcome of the system owing to failure in system downtown. It has been observed that two elements influence enterprises owing to worthwhile threat assault due to successful threat attacks. Therefore, system consolidation engenders a performance acquired from the system's actual performance. In the assault-linked system collapse, the influence is observed in two layers - decline in output and average expenditure for preservation or to create a system of natural assault, as shown in figure 19.

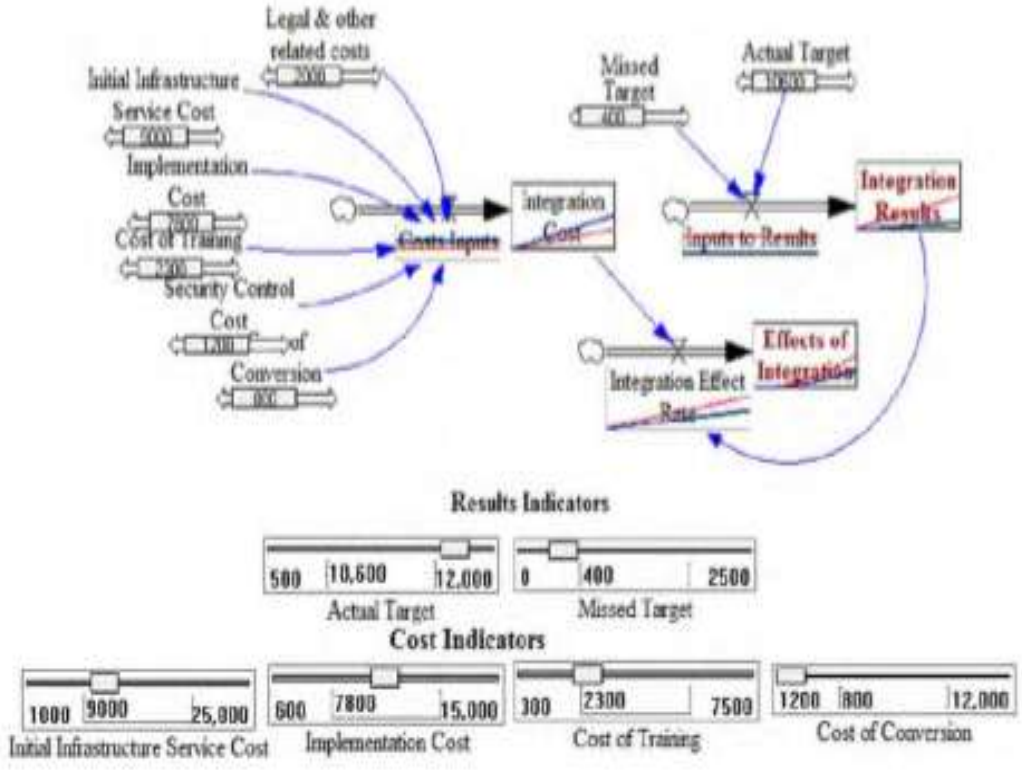

Figure 19:- Business impact of Attack.

Safety hazard exposure simulation

Based on Equation 4, the risk is believed to be the outcome of probability and the influence of assault, such as R = L * I, which is described in Figure 20. System risk exposure is fascinated with the maintenance of fundamentals with the aid of sliders coupled with the corresponding variable. It has been observed that movement of slider is connected with systems susceptibility to the right such as escalation in susceptibility range of system results in rising of threat exposure of system that leads to the escalation in the probability of threat towards assault.

Results and hypothesis:-

It entails examining the models to accommodate either to reproduce the vitality, the system they reflect, or to examine the assumption. In addition, another crucial examination related to the confirmation to ascertain in case system and subsystems posses the worthiness context to realistic conditions.

Test Results

The simulation operative utilizes four groups of measurement combinations to examine the probability of risk assault. These are:

➢ The greater threat levels lead to the lower level of susceptibility and feebleness SCs. ➢ A more level of threat leads to higher susceptibility and weakness SCs ➢ High threat levels, high susceptibility, and potent SCs ➢ The more level of threat range leads to a decline in susceptibility and an increase in SCs

The simulation strategy authorizes the modeller to acquire an extensive perspective or comprehension of system conduct from various scenarios and to consider or offer alteration in policies to the present approaches for action-based methodologies. As shown in Figure 21, simulation operates by utilizing the below measurements with adjustable inputs in the table

• INITIAL TIME (initial time for the simulation) = 1 month
• FINAL TIME (Final time for the simulation) = 12 months
• TIME STEP (Time step for the simulation) = 0.0078125 months. The time step of 0.0078 months was accustomed to offering smooth time outlines for the various measurements in the model.

The result is described in Figure 21, which reflects the possibility of high threat associated assaults while the susceptibility range is more with a weak level of SCs. It has been represented with the help of Test 2 on the simulation graph. However, Test 3 (Strong SCs) reflect upon different scenarios while threat and susceptibility are considered more. Potent SCs counterbalance the influence owing to both risk and susceptibility ranges in Test 3. A lower level of possibility in Scenarios is found while declining in susceptibility and robust range of SCs. Test 4 shows a lower level of possibility against threat assault. With the utilization of similar measurements, the influence of threat attacks in the context of enterprises has been noticed with the aid of maintenance in system value. The test is being operated with the help of two supplementary combinations—test V: Right lower value system and Test VI: Appropriate higher system Value. As shown in Figure 22, the results lead to the representation of two extreme scenarios, which result in equal chance in the context of a threat attack. However, the potent influence of system collapse is high while system value is more. The model represented beyond has not been created for specific technological applications. The measurement being utilized in the simulation process was operator inputs from the Small and Medium-sized enterprises. Various groups of measurements are needed for the specific technical solution.

The simulation operates for twelve months which is considered the time frame for the technology integration procedure. The introductory month value is attributed to 1 and a time step value of 0.0078125.

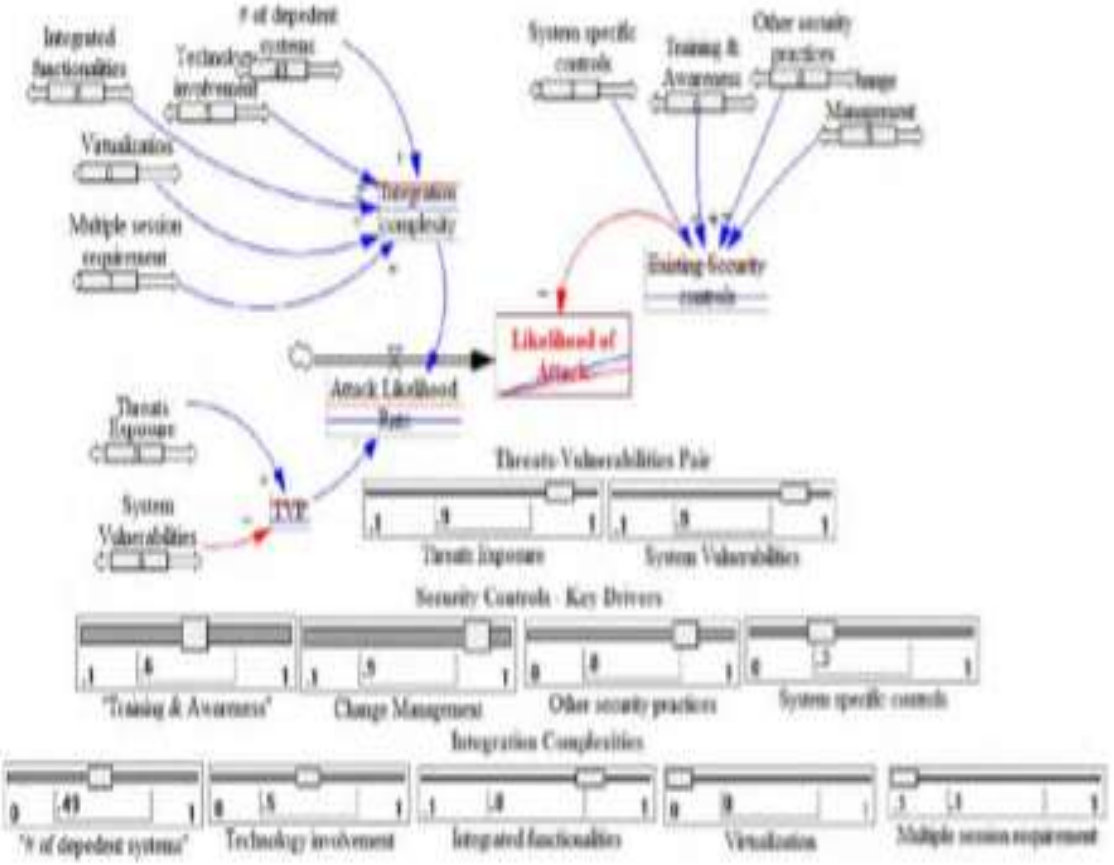

Figure 20:- Screenshot of Likelihood of Attack (with control).

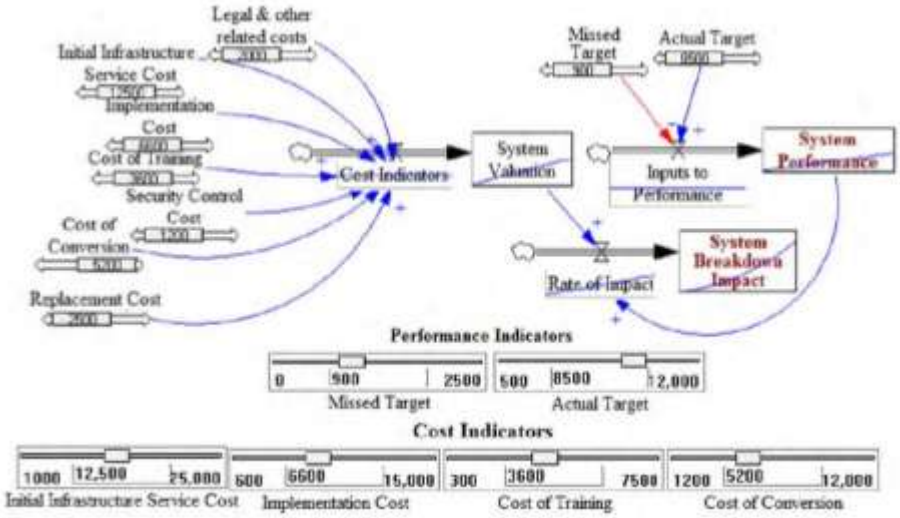

Figure 21:- Screenshot of the Impact attack.

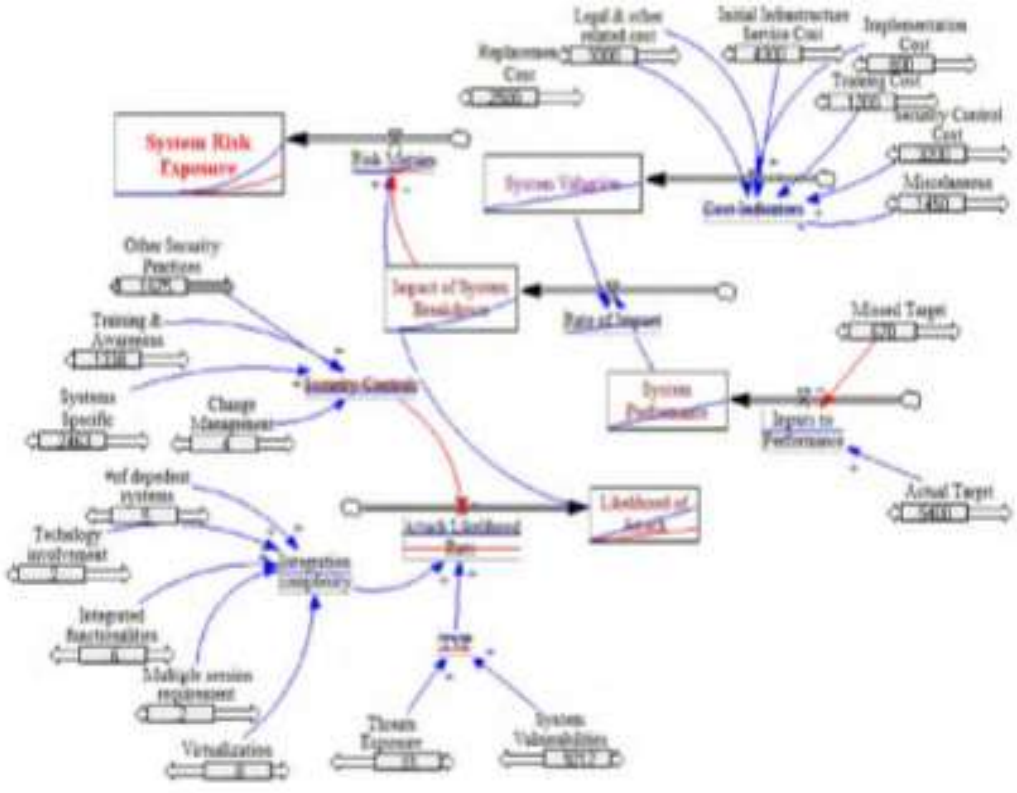

Figure 22:- Screenshot of system risk exposure.

Chapter 5:

Conclusion:-

An insignificant percentage of published writings is turned out to possess a crucial safety structure from dynamic system modelling. It has been observed that several pieces of research regarding prescribed techniques are associated with fear or susceptibility recognition. A metric identification scheme is undoubtedly worthwhile for elaborating a theoretical basis; however, observed as a concern based on quite a prediction and quantification of behavioural features related to system and subsystem as described in Equation 4, which is observed as an unexpected one. From which aspect, strategy has been designed in this study. Evaluation of safety risk under

supervised conditions is considered intuitive based on facts. The contemporary strategy must feature quantities and qualities that are intrinsically unpredictable and troublesome for quantification. It has been explored that critical structural systems and assisted techniques have become intricated and dynamics with the intent to forecast owing to the concurrence in modern technologies. Likewise, the confinement of the system is shown to have difficulty in definition due to the codependence of systems. The enterprise influences coupled with significant threat assault on crucial structural system leads to be highly determinantal not for system only but to codependencies and well being of city dwellers. Based on the review, it has been observed the presence of several safety-associated threats evaluation strategies. However, the intricacies and rises in inter reliance of contemporary crucial systems depict the present evaluation strategy as worthless.

Consequently, there is a requirement to cultivate various safety risk assessment strategies to address the lacunas among current methodologies because no comprehensive approach is observed against safety-associated concerns. To conclude, it has been seen that both modelling and simulation are illustrated in the research for specifical assessment of safety-linked risk with the aid of controlled techniques accountable for the encouragement of critical structural systems such as power distribution. To develop modelling strategies, seven prime assessment metrics were evaluated. System characterization follows the controlled techniques of ISCSSCADA. Undoubtedly, the strategy emphasizes crucial structural systems. However, it offers the capability to evaluate the respective strength of various crucial system contributions for clients, regulatory agencies, resource owners, and vendors.

References:-

1. Bakıcı, T., Almirall, E., Wareham, J., 2013. A smart city initiative: the case of Barcelona. J. Knowl. Econ. 4, 135–148.
2. Denhardt, J.V., Denhardt, R.B., 2015. The new public service: Serving, not steering. Routledge
3. Taylor Buck, N., While, A., 2017. Competitive urbanism and the limits to smart city innovation: The UK Future Cities initiative. Urban Stud. 54, 501–519.
4. Hellsten, P., Pekkola, S., 2019. The Impact Levels of Digitalization Initiatives. EGOV-CeDEM-EPart 2019 109.
5. Hellsten, P., Pekkola, S., 2019. The Impact Levels of Digitalization Initiatives. EGOV-CeDEM-EPart 2019 109
6. Helander, N., Jussila, J., Bal, A., Sillanpää, V., Paunu, A., Ammirato, S., Felicetti, A., 2020. Co-creating Digital Government sSrvice: An Activity Theory Perspective, in: Proceedings of the 53rd Hawaii International Conference on System Science
7. Lupapiste [WWW Document], n.d. URL https://www.lupapiste.fi/ (accessed 6.15.20).
8. Vartolomei, V.C. and Avasilcai, S., 2019, August. Challenges of digitalization process in different industries. Before and after. In IOP Conference Series: Materials Science and Engineering (Vol. 568, No. 1, p. 012086). IOP Publishing.
9. Kharlamova, N., Hashemi, S. and Træholt, C., 2021. Data-driven approaches for cyber defense of battery energy storage systems. Energy and AI, 5, p.100095.
10. Lee, C., Chae, Y.H. and Seong, P.H., 2021. Development of a method for estimating security state: Supporting integrated response to cyber-attacks in NPPs. Annals of Nuclear Energy, 158, p.108287.
11. Qiu, W., Sun, K., Yao, W., You, S., Yin, H., Ma, X. and Liu, Y., 2021. Time-frequency based cyber security defense of wide-area control system for fast frequency reserve. International Journal of Electrical Power & Energy Systems, 132, p.107151.
12. Zhang, Y. and Malacaria, P., 2021. Bayesian Stackelberg games for cyber-security decision support. Decision Support Systems, 148, p.113599.
13. Kim, Y.S., Choi, M.K., Han, S.M., Lee, C. and Seong, P.H., 2020. Development of a method for quantifying relative importance of NPP cyber attack probability variables based on factor analysis and AHP. Annals of Nuclear Energy, 149, p.107790.
14. Hacioglu, U. and Sevgilioglu, G., 2019. The evolving role of automated systems and its cyber-security issue for global business operations in Industry 4.0. International Journal of Business Ecosystem & Strategy (2687-2293), 1(1), pp.01-11.
15. Eling, M. and Lehmann, M., 2018. The impact of digitalization on the insurance value chain and the insurability of risks. The Geneva papers on risk and insurance-issues and practice, 43(3), pp.359-396.
16. Bryzgalov, D.V., Gryzenkova, Y.V. and Tsyganov, A.A., 2020. Prospects for Digitalization of the Insurance Business in Russia. Financial Journal, 12(3), pp.76-90.
17. Tosun, O.K., 2021. Cyber-attacks and stock market activity. International Review of Financial Analysis, 76, p.101795.

18. Ogbanufe, O., 2021. Enhancing end-user roles in information security: exploring the setting, situation, and identity. Computers & Security, 108, p.102340.
19. Alkatheiri, M.S., Chauhdary, S.H. and Alqarni, M.A., 2021. Seamless security apprise method for improving the reliability of sustainable energy-based smart home applications. Sustainable Energy Technologies and Assessments, 45, p.101219.
20. Krishnasamy, V. and Venkatachalam, S., 2021. An efficient data flow material model based cloud authentication data security and reduce a cloud storage cost using Index-level Boundary Pattern Convergent Encryption algorithm. Materials Today: Proceedings.
21. Palmieri, M., Shortland, N. and McGarry, P., 2021. Personality and online deviance: The role of reinforcement sensitivity theory in cybercrime. Computers in human behavior, 120, p.106745.
22. Le Nguyen, C. and Golman, W., 2021. Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries:'Law on the books' vs 'law in action'. Computer Law & Security Review, 40, p.105521.
23. Chandra, A. and Snowe, M.J., 2020. A taxonomy of cybercrime: Theory and design. International Journal of Accounting Information Systems, 38, p.100467.
24. Katrakazas, C., Theofilatos, A., Papastefanatos, G., Härri, J. and Antoniou, C., 2020. Cyber security and its impact on CAV safety: Overview, policy needs and challenges. Advances in Transport Policy and Planning, 5, pp.73-94.
25. Tam, T., Rao, A. and Hall, J., 2021. The good, the bad and the missing: A Narrative review of cyber-security implications for australian small businesses. Computers & Security, 109, p.102385.
26. Cheng, S., Zhao, G., Gao, M., Shi, Y., Huang, M. and Marefati, M., 2021. A new hybrid solar photovoltaic/phosphoric acid fuel cell and energy storage system; Energy and Exergy performance. International Journal of Hydrogen Energy, 46(11), pp.8048-8066.
27. Alghamdie, M.I., 2021. A novel study of preventing the cyber security threats. Materials Today: Proceedings.
28. Quigley, K., Burns, C. and Stallard, K., 2015. 'Cyber Gurus': A rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection. Government Information Quarterly, 32(2), pp.108-117.
29. Sakhnini, J., Karimipour, H., Dehghantanha, A. and Parizi, R.M., 2021. Physical layer attack identification and localization in cyber–physical grid: An ensemble deep learning based approach. Physical Communication, 47, p.101394.
30. Baig, Z.A., Szewczyk, P., Valli, C., Rabadia, P., Hannay, P., Chernyshev, M., Johnstone, M., Kerai, P., Ibrahim, A., Sansurooah, K. and Syed, N., 2017. Future challenges for smart cities: Cyber-security and digital forensics. Digital Investigation, 22, pp.3-13.
31. Arend, I., Shabtai, A., Idan, T., Keinan, R. and Bereby-Meyer, Y., 2020. Passive-and not active-risk tendencies predict cyber security behavior. Computers & Security, 97, p.101964.
32. Hart, S., Margheri, A., Paci, F. and Sassone, V., 2020. Riskio: A serious game for cyber security awareness and education. Computers & Security, 95, p.101827.
33. Ensley, M.R., 1995. Toward a theory of situation awareness in dynamic systems. Human factors, 37, pp.85-104.
34. Ma, L., Zhang, Y., Yang, C. and Zhou, L., 2021. Security control for two-time-scale cyber physical systems with multiple transmission channels under DoS attacks: The input-to-state stability. Journal of the Franklin Institute, 358(12), pp.6309-6325.
35. Jamal, A.A., Majid, A.A.M., Konev, A., Kosachenko, T. and Shelupanov, A., 2021. A review on security analysis of cyber physical systems using Machine learning. Materials Today: Proceedings.
36. Rodríguez-deArriba, M.L., Nocentini, A., Menesini, E. and Sánchez-Jiménez, V., 2021. Dimensions and measures of cyber dating violence in adolescents: A systematic review. Aggression and Violent Behavior, 58, p.101613.
37. Thomson, J.R., 2015. Cyber security, cyber-attack and cyber-espionage. High Integrity Systems and Safety Management in Hazardous Industries, pp.45-53.
38. Khan, S.K., Shiwakoti, N., Stasinopoulos, P. and Chen, Y., 2020. Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions. Accident Analysis & Prevention, 148, p.105837.
39. Furnell, S. and Shah, J.N., 2020. Home working and cyber security–an outbreak of unpreparedness?. Computer fraud & security, 2020(8), pp.6-12.
40. Mehrpooya, M., Ghadimi, N., Marefati, M. and Ghorbanian, S.A., 2021. Numerical investigation of a new combined energy system includes parabolic dish solar collector, Stirling engine and thermoelectric device. International Journal of Energy Research, 45(11), pp.16436-16455.

41. Alibasic, A., Al Junaibi, R., Aung, Z., Woon, W.L. and Omar, M.A., 2016, September. Cybersecurity for smart cities: A brief review. In International Workshop on Data Analytics for Renewable Energy Integration (pp. 22-30). Springer, Cham.
42. Yang, S.H., Cao, Y., Wang, Y., Zhou, C., Yue, L. and Zhang, Y., 2021. Harmonizing safety and security risk analysis and prevention in cyber-physical systems. Process safety and environmental protection, 148, pp.1279-1291.
43. Zhao, J., Yan, Q., Li, J., Shao, M., He, Z. and Li, B., 2020. TIMiner: Automatically extracting and analyzing categorized cyber threat intelligence from social data. Computers & Security, 95, p.101867.
44. Zhao, Z.G., Ye, R.B., Zhou, C., Wang, D.H. and Shi, T., 2021. Control-theory based security control of cyber-physical power system under multiple cyber-attacks within unified model framework. Cognitive Robotics, 1, pp.41-57.
45. Motsch, W., David, A., Sivalingam, K., Wagner, A. and Ruskowski, M., 2020. Approach for dynamic price-based demand side management in cyber-physical production systems. Procedia manufacturing, 51, pp.1748-1754.
46. Cao, Y., Huang, Z., Ke, C., Xie, J. and Wang, J., 2019. A topology-aware access control model for collaborative cyber-physical spaces: Specification and verification. Computers & security, 87, p.101478.
47. Zou, T., Bretas, A.S., Ruben, C., Dhulipala, S.C. and Bretas, N., 2020. Smart grids cyber-physical security: Parameter correction model against unbalanced false data injection attacks. Electric power systems research, 187, p.106490.
48. Robinson, M., Jones, K. and Janicke, H., 2015. Cyber warfare: Issues and challenges. Computers & security, 49, pp.70-94.
49. Edgar, T. and Manz, D., 2017. Research methods for cyber security. Syngress.
50. Nicholson, A., Webber, S., Dyer, S., Patel, T. and Janicke, H., 2012. SCADA security in the light of Cyber-Warfare. Computers & Security, 31(4), pp.418-436.
51. Quigley, K., Burns, C. and Stallard, K., 2015. 'Cyber Gurus': A rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection. Government Information Quarterly, 32(2), pp.108-117.
52. Damon, E., Mache, J., Weiss, R., Ganz, K., Humbeutel, C. and Crabill, M., 2014. Cyber Security Education: The Merits of Firewall Exercises. In Emerging Trends in ICT Security (pp. 507-516). Morgan Kaufmann.
53. Shamel, A., Marefati, M., Alayi, R., Gholaminia, B. and Rohl, H., 2016. Designing a PID controller to control a fuel cell voltage using the imperialist competitive algorithm. Advances in Science and Technology. Research Journal, 10(30).
54. Varga, S., Brynielsson, J. and Franke, U., 2021. Cyber-threat perception and risk management in the Swedish financial sector. Computers & Security, 105, p.102239.
55. Bullock, J.A., Haddow, G.D. and Coppola, D.P., 2021. Cybersecurity and critical infrastructure protection. Introduction to Homeland Security, pp.425-497.
56. Chen, J.K., Chang, C.W., Wang, Z., Wang, L.C. and Wei, H.S., 2021. Cyber deviance among adolescents in Taiwan: Prevalence and correlates. Children and Youth Services Review, 126, p.106042.
57. Iqbal, Z. and Anwar, Z., 2020. SCERM—A novel framework for automated management of cyber threat response activities. Future Generation Computer Systems, 108, pp.687-708.
58. Patel, D.C., Berry, M.F., Bhandari, P., Backhus, L.M., Raees, S., Trope, W., Nash, A., Lui, N.S., Liou, D.Z. and Shrager, J.B., 2021. Paradoxical Motion on Sniff Test Predicts Greater Improvement Following Diaphragm Plication. The Annals of Thoracic Surgery, 111(6), pp.1820-1826.
59. Aziz, A.A. and Amtul, Z., 2019. Developing Trojan horses to induce, diagnose and suppress Alzheimer's pathology. Pharmacological Research, 149, p.104471
60. Al Shaer, D., Al Musaimi, O., Beatriz, G. and Albericio, F., 2020. Hydroxamate siderophores: Natural occurrence, chemical synthesis, iron binding affinity and use as Trojan horses against pathogens. European Journal of Medicinal Chemistry, 208, p.112791.
61. Zhang, Y. and Malacaria, P., 2021. Bayesian Stackelberg games for cyber-security decision support. Decision Support Systems, 148, p.113599.
62. Beechey, M., Kyriakopoulos, K.G. and Lambotharan, S., 2021. Evidential classification and feature selection for cyber-threat hunting. Knowledge-Based Systems, 226, p.107120.
63. Solomon, R., 2017. Electronic protests: Hacktivism as a form of protest in Uganda. Computer law & security review, 33(5), pp.718-728.
64. Saxena, R. and Gayathri, E., 2022. Cyber threat intelligence challenges: Leveraging blockchain intelligence with possible solution. Materials Today: Proceedings, 51, pp.682-689.

65. Topping, C., Dwyer, A., Michalec, O., Craggs, B. and Rashid, A., 2021. Beware suppliers bearing gifts!: Analysing coverage of supply chain cyber security in critical national infrastructure sectorial and cross-sectorial frameworks. Computers & Security, 108, p.102324.
66. Marefati, M., Mehrpooya, M. and Shafii, M.B., 2018. Optical and thermal analysis of a parabolic trough solar collector for production of thermal energy in different climates in Iran with comparison between the conventional nanofluids. Journal of cleaner production, 175, pp.294-313.
67. Li, J., Sun, C. and Su, Q., 2021. Analysis of cascading failures of power cyber-physical systems considering false data injection attacks. Global Energy Interconnection, 4(2), pp.204-213.
68. Alghamdi, M.I., 2021. Determining the impact of cyber security awareness on employee behaviour: A case of Saudi Arabia. Materials Today: Proceedings.
69. Sun, C.C., Hahn, A. and Liu, C.C., 2018. Cyber security of a power grid: State-of-the-art. International Journal of Electrical Power & Energy Systems, 99, pp.45-56.
70. Assessment, R., 2010. Mapping Guidelines for Disaster Management. European Commission, SEC, 1626.
71. Giannopoulos, G., Filippini, R. and Schimmer, M., 2012. Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art. JRC Technical Notes, 1(1), pp.1-53.
72. European Commission, 2014. Overview of Natural and Man-Made Disaster Risks in the EU. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. The Post-2015 Hyogo Framework for Action: Managing Risks to Achieve Resilience.
73. Directive, C., 2008. 114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Official Journal of the European Union, 23, p.2008.
74. Udeanu, G., 2015, June. A New Approach To The European Programme For Critical Infrastructure Protection. In International conference KNOWLEDGE-BASED ORGANIZATION (Vol. 21, No. 1, pp. 135-142).
75. Galbusera, L., Giannopoulos, G. and Ward, D., 2014. Developing stress tests to improve the resilience of critical infrastructures: a feasibility analysis. European commission JRC91129 EUR, 26971.
76. .Council, E.U., 2010. The Stockholm Programme—An open and secure Europe serving and protecting citizens. Official Journal of the European Union, pp.1-38.
77. .Horjan, A.M. and Šuperina, M., 2012. The EU Internal Security Strategy in Action: Five steps towards a moor secure Europe. Policijaisigurnost, 21(1), pp.70-104.
78. .Carpignano, A., Grosso, D., Gerboni, R. and Bologna, A., 2020. Resilience of Critical Infrastructures: A Risk Assessment Methodology for Energy Corridors. In Issues on Risk Analysis for Critical Infrastructure Protection. IntechOpen.
79. EU Commission, 2004. Critical Infrastructure Protection in the fight against terrorism.
80. .EU Commission, 2006. Communication from the commission on a european programme for critical infrastructure protection. COM (2006), 786.
81. .Udeanu, G., 2015, June. A New Approach To The European Programme For Critical Infrastructure Protection. In International conference KNOWLEDGE-BASED ORGANIZATION (Vol. 21, No. 1, pp. 135-142).
82. European Commission. Evaluation study of Council Directive 2008/114 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Final Report
83. Ouyang, M., 2014. Review on modeling and simulation of interdependent critical infrastructure systems. Reliability engineering & System safety, 121, pp.43-60.
84. Griot, C., 2010. Modelling and simulation for critical infrastructure interdependency assessment: a meta-review for model characterisation. International journal of critical infrastructures, 6(4), pp.363-379.
85. Wang, S., Hong, L., Chen, X., Zhang, J. and Yan, Y., 2011, July. Review of interdependent infrastructure systems vulnerability analysis. In 2011 2nd International Conference on Intelligent Control and Information Processing (Vol. 1, pp. 446-451). IEEE.
86. Liu, W. and Song, Z., 2020. Review of studies on the resilience of urban critical infrastructure networks. Reliability Engineering & System Safety, 193, p.106617.
87. Galbusera, L., Giannopoulos, G. and Ward, D., 2014. Developing stress tests to improve the resilience of critical infrastructures: a feasibility analysis. European commission JRC91129 EUR, 26971.
88. Giannopoulos, G., Filippini, R. and Schimmer, M., 2012. Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art. JRC Technical Notes, 1(1), pp.1-53.
89. Haimes, Y.Y., 2008. Models for risk management of systems of systems. International Journal of System of Systems Engineering, 1(1-2), pp.222-236.
90. Pinto, C.A., McShane, M.K. and Bozkurt, I., 2012. System of systems perspective on risk: towards a unified concept. International Journal of System of Systems Engineering, 3(1), pp.33-46.

91. Eusgeld, I., Nan, C. and Dietz, S., 2011. "System-of-systems" approach for interdependent critical infrastructures. Reliability Engineering & System Safety, 96(6), pp.679-686.
92. Labaka, L., Hernantes, J. and Sarriegi, J.M., 2015. Resilience framework for critical infrastructures: An empirical study in a nuclear plant. Reliability Engineering & System Safety, 141, pp.92-105.
93. Labaka, L., Hernantes, J. and Sarriegi, J.M., 2016. A holistic framework for building critical infrastructure resilience. Technological Forecasting and Social Change, 103, pp.21-33.
94. Mao, Q., Li, N. and Peña-Mora, F., 2019. Quality function deployment-based framework for improving the resilience of critical infrastructure systems. International Journal of Critical Infrastructure Protection, 26, p.100304.
95. Nan, C. and Sansavini, G., 2017. A quantitative method for assessing resilience of interdependent infrastructures. Reliability Engineering & System Safety, 157, pp.35-53.
96. Ouyang, M., Liu, C. and Xu, M., 2019. Value of resilience-based solutions on critical infrastructure protection: Comparing with robustness-based solutions. Reliability Engineering & System Safety, 190, p.106506.
97. Theocharidou, M. and Giannopoulos, G., 2015. Risk assessment methodologies for critical infrastructure protection. Part II: A new approach, Luxembourg: Publications Office of the European Union.
98. Choi, H.Y., Kim, K.M., Han, J., Sah, S., Kim, S.H., Hwang, S.H., Lee, K.N., Pyun, J.K., Montmayeur, N., Marca, C. and Haug, E., 2007, July. Human body modeling for riding comfort simulation. In International Conference on Digital Human Modeling (pp. 813-823). Springer, Berlin, Heidelberg.
99. Ferrario, E., Pedroni, N. and Zio, E., 2016. Evaluation of the robustness of critical infrastructures by Hierarchical Graph representation, clustering and Monte Carlo simulation. Reliability Engineering & System Safety, 155, pp.78-96
100. Kröger, R., 2011. Studien-und Lebenspraxis internationaler und deutscher Studierender: Erfahrungen bei der Ausbildung eines ingenieurwissenschaftlichen Habitus. Springer-Verlag.
101. Zio, E., 2016. Critical infrastructures vulnerability and risk analysis. European Journal for Security Research, 1(2), pp.97-114.
102. Zio, E., 2016. Challenges in the vulnerability and risk analysis of critical infrastructures. Reliability Engineering & System Safety, 152, pp.137-150.
103. Johansson, J., Hassel, H. and Zio, E., 2013. Reliability and vulnerability analyses of critical infrastructures: Comparing two approaches in the context of power systems. Reliability Engineering & System Safety, 120, pp.27-38.
104. Johansson, J. and Hassel, H., 2010. An approach for modelling interdependent infrastructures in the context of vulnerability analysis. Reliability Engineering & System Safety, 95(12), pp.1335-1344.
105. Stergiopoulos, G., Kotzanikolaou, P., Theocharidou, M. and Gritzalis, D., 2015. Risk mitigation strategies for critical infrastructures based on graph centrality analysis. International Journal of Critical Infrastructure Protection, 10, pp.34-44.
106. Kotzanikolaou, P., Theoharidou, M. and Gritzalis, D., 2013, March. Cascading effects of common-cause failures in critical infrastructures. In International Conference on Critical Infrastructure Protection (pp. 171-182). Springer, Berlin, Heidelberg.
107. Stergiopoulos, G., Kotzanikolaou, P., Theocharidou, M., Lykou, G. and Gritzalis, D., 2016. Time-based critical infrastructure dependency analysis for large-scale and cross-sectoral failures. International Journal of Critical Infrastructure Protection, 12, pp.46-60.
108. .Kotzanikolaou, P., Theoharidou, M. and Gritzalis, D., 2011, September. Interdependencies between critical infrastructures: Analyzing the risk of cascading effects. In International Workshop on Critical Information Infrastructures Security (pp. 104-115). Springer, Berlin, Heidelberg.
109. Fu, G., Khoury, M., Dawson, R. and Bullock, S., 2013. Vulnerability analysis of interdependent infrastructure systems. In Proceedings of the European Conference on Complex Systems 2012 (pp. 317-323). Springer, Cham.
110. Utne, I.B., Hokstad, P. and Vatn, J., 2011. A method for risk modeling of interdependencies in critical infrastructures. Reliability Engineering & System Safety, 96(6), pp.671-678.
111. .Azzini, I., Dido, M., Giannopoulos, G. and Galbusera, L., 2016. GRRASP version 3.1 User Manual. Luxembourg: Publications Office of the European Union, pp.93-110.
112. Kostyaeva, E.V. and Chernyakov, M.K., 2020, December. Factors of Development of Insurance of Small and Medium-Sized Businesses in the Conditions of Digitalization. In 2nd International Scientific and Practical Conference on Digital Economy (ISCDE 2020) (pp. 417-423). Atlantis Press.
113. Cappiello, C., Meroni, G., Pernici, B., Plebani, P., Salnitri, M., Vitali, M., Trojaniello, D., Catallo, I. and Sanna, A., 2020. Improving health monitoring with adaptive data movement in fog computing. Frontiers in Robotics and AI, 7, p.96.

114.,Paquette, S., Jaeger, P.T. and Wilson, S.C., 2010. Identifying the security risks associated with governmental use of cloud computing. Government information quarterly, 27(3), pp.245-253.
115. Stoneburner, G., Goguen, A. and Feringa, A., 2002. Risk management guide for information technology systems. Nist special publication, 800(30), pp.800-30.
116. Kaplan, S. and Garrick, B.J., 1981. On the quantitative definition of risk. Risk analysis, 1(1), pp.11-27.
117. De Bruijne, M. and Van Eeten, M., 2007. Systems that should have failed: critical infrastructure protection in an institutionally fragmented environment. Journal of contingencies and crisis management, 15(1), pp.18-29.
118. Pieters, W., 2011. The (social) construction of information security. The Information Society, 27(5), pp.326-335.
119. Wei, Y.M., Fan, Y., Lu, C. and Tsai, H.T., 2004. The assessment of vulnerability to natural disasters in China by using the DEA method. Environmental Impact Assessment Review, 24(4), pp.427-439.
120. Dahbur, K., Mohammad, B. and Tarakji, A.B., 2011, April. A survey of risks, threats and vulnerabilities in cloud computing. In Proceedings of the 2011 International conference on intelligent semantic Web-services and applications (pp. 1-6).
121. Johansson, J., Hassel, H. and Cedergren, A., 2011. Vulnerability analysis of interdependent critical infrastructures: case study of the Swedish railway system. International journal of critical infrastructures, 7(4), pp.289-316.
122. Touhill, G.J. and Touhill, C.J., 2014. Cybersecurity for executives: A practical guide. John Wiley & Sons.
123. Johansson, J., 2010. Risk and vulnerability analysis of interdependent technical infrastructures. Lund University, Dept. of Measurement Technology and Industrial Electrical Engineering.
124. Apostolakis, G.E. and Lemon, D.M., 2005. A screening methodology for the identification and ranking of infrastructure vulnerabilities due to terrorism. Risk Analysis: An International Journal, 25(2), pp.361-376.
125. Latora, V. and Marchiori, M., 2005. Vulnerability and protection of infrastructure networks. Physical Review E, 71(1), p.015103.
126. Forrester, J.W., 2003. Dynamic models of economic systems and industrial organizations. System Dynamics Review: The Journal of the System Dynamics Society, 19(4), pp.329-345.
127. Silver, E. and Miller, L.L., 2002. A cautionary note on the use of actuarial risk assessment tools for social control. Crime & Delinquency, 48(1), pp.138-161.
128. Sterman, J., 2002. System Dynamics: systems thinking and modeling for a complex world.
129. Rinaldi, S.M., Peerenboom, J.P. and Kelly, T.K., 2001. Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE control systems magazine, 21(6), pp.11-25.
130. Appari, A. and Johnson, M.E., 2010. Information security and privacy in healthcare: current state of research. International journal of Internet and enterprise management, 6(4), pp.279-314.
131. Bloomfield, R.E., Popov, P., Salako, K., Stankovic, V. and Wright, D., 2017. Preliminary interdependency analysis: An approach to support critical-infrastructure risk-assessment. Reliability Engineering & System Safety, 167, pp.198-217.
132. Bodin, L.D., Gordon, L.A. and Loeb, M.P., 2008. Information security and risk management. Communications of the ACM, 51(4), pp.64-68.
133. Crouchy, M., Galai, D. and Mark, R., 2006. Risk management–a helicopter view. The Essentials of Risk Management, edited by M. Crouhy, D. Galai and R. Mark. New York: McGraw-Hill, pp.1-36.
134. Ebrahimi, B., Tafreshi, R., Mohammadpour, J., Franchek, M., Grigoriadis, K. and Masudi, H., 2013. Second-order sliding mode strategy for air–fuel ratio control of lean-burn SI engines. IEEE Transactions on Control Systems Technology, 22(4), pp.1374-1384.
135. Hassel, H., 2010. Risk and vulnerability analysis in society's proactive emergency management: Developing methods and improving practices.
136. Kaliski Jr, B.S. and Pauley, W., 2010a. Toward risk assessment as a service in cloud environments. In 2nd USENIX Workshop on Hot Topics in Cloud Computing (HotCloud 10).
137. Kaliski Jr, B.S. and Pauley, W., 2010.b Toward risk assessment as a service in cloud environments. In 2nd USENIX Workshop on Hot Topics in Cloud Computing (HotCloud 10).
138. Little, R.G., 2002. Controlling cascading failure: Understanding the vulnerabilities of interconnected infrastructures. Journal of Urban Technology, 9(1), pp.109-123.
139. Bush, G.W., 2003. National strategy for the physical protection of critical infrastructures and key assets. Department of Homeland Security.
140. Ozier, W., 1999. A framework for an automated risk assessment tool. Retrieved January, 25, p.2007.
141. Paté-Cornell, M.E., Kuypers, M., Smith, M. and Keller, P., 2018. Cyber risk management for critical infrastructure: a risk analysis model and three case studies. Risk Analysis, 38(2), pp.226-241.

142. Rinaldi, S.M., 2004, January. Modeling and simulating critical infrastructures and their interdependencies. In 37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of the (pp. 8-pp). IEEE.
143. Sangroya, A., Kumar, S., Dhok, J. and Varma, V., 2010, March. Towards analyzing data security risks in cloud computing environments. In International Conference on Information Systems, Technology and Management (pp. 255-265). Springer, Berlin, Heidelberg.
144. Sawyer, S. and Jarrahi, M.H., 2014. Sociotechnical approaches to the study of information systems. In Computing handbook, third edition: Information systems and information technology (pp. 5-1). CRC Press.
145. Schuetze, W.P., 1993. What is an Asset?. Accounting horizons, 7(3), p.66.
146. TheSecurityRiskManagementGuide-Microsoft.pdf, n.d.
147. Van Deursen, N., Buchanan, W.J. and Duff, A., 2013. Monitoring information security risks within health care. computers & security, 37, pp.31-45.
148. Zhang, X., Wuwong, N., Li, H. and Zhang, X., 2010, June. Information security risk management framework for the cloud computing environments. In 2010 10th IEEE international conference on computer and information technology (pp. 1328-1334). IEEE.
149. Zimmerman, R., 2001. Social implications of infrastructure network interactions. Journal of Urban Technology, 8(3), pp.97-119.