Cyber Security and Its Vulnerability

Tripti Gupta, Nischal Sharma, Riya Sharma and Sarita Garg

Jaipur Engineering College and Research Centre, Jaipur, INDIA

Abstract:

The level of protection of high voltage power substations depends on the considerations of the electricity company, the level of threats and the value of their assets. On the other hand, the level of countermeasures or defences for an acceptable level of risk depends on the number of defence equipment at the substation level. Therefore, the number of these countermeasures should be estimated according to the status of each substation and the rate of investment and its importance. In addition, appropriate defence methods depending on their type and condition, as well as how the design and position of the substation can identify system security vulnerabilities. The aim of this paper is to investigate and determine the importance of protecting high voltage power substations against cyber-attacks. For this purpose, power substations are examined in four different groups: geostrategic, industrial strategy, automation and control systems, and vulnerable. According to the decision-making method of Fuzzy Analytical Hierarchy Process (FAHP), the defence cost function is presented in each substation, which includes hardware and software equipment and optimal routing of data transmission cables and cable shield. In addition, decisions are made simultaneously between the defender and the attacker. It was found that, from the proposed defence methods, the optimal path for communication cables and hardware equipment used in the power substations was more important than other cases. In addition, by shifting the weights of the criteria of substations 2 and 4, the strategy 3 ranks first in the need for defence budgets among other strategies, accounting for about 49.5% of the total defence budget, and it needs 11.2% more defence budget than the strategy S4. Furthermore, sensitivity analysis is provided to examine the impact of various factors as well as to confirm the accuracy of the results.

Keywords: Information technology, Cyber-attacks, Cyber security, Emerging trends, Key management

Introduction : Globalisation, digitalisation and smart technologies have escalated the propensity and severity of cybercrime. Whilst it is an emerging field of research and industry, the importance of robust cybersecurity defence systems has been highlighted at the corporate, national and supranational levels. The impacts of inadequate cybersecurity are estimated to have cost the global economy USD 945 billion in 2020. Cyber vulnerabilities pose significant corporate risks, including business interruption, breach of privacy and financial losses. Despite the increasing relevance for the international economy, the availability of data on cyber risks remains limited. The reasons for this are many. Firstly, it is an emerging and evolving risk; therefore, historical data sources are limited. It could also be due to the fact that, in general, institutions that have been hacked do not publish the incidents. The lack of data poses challenges for many areas, such as research, risk management and cybersecurity. The importance of this topic is demonstrated by the announcement of the European Council in April 2021 that a centre of excellence for cybersecurity will be established to pool investments in research, technology and industrial development. The goal of this centre is to increase the security of the internet and other critical network and information systems.

This research takes a risk management perspective, focusing on cyber risk and considering the role of cybersecurity and cyber insurance in risk mitigation and risk transfer. The study reviews the existing literature and open data sources related to cybersecurity and cyber risk. This is the first systematic review of data availability in the general context of cyber risk and cybersecurity. By identifying and critically analysing the available datasets, this paper supports the research community by aggregating, summarising and categorising all available open datasets. In addition, further information on datasets is attached to provide deeper insights and support stakeholders engaged in cyber risk control and cybersecurity. Finally, this research paper highlights the need for open access to cyber-specific data, without price or permission barriers.

The identified open data can support cyber insurers in their efforts on sustainable product development. To date, traditional risk assessment methods have been untenable for insurance companies due to the absence of historical claims data. These high levels of uncertainty mean that cyber insurers are more inclined to overprice cyber risk cover. Combining external data with insurance portfolio data therefore seems to be essential to improve the evaluation of the risk and thus lead to risk-adjusted pricing. This argument is also supported by the fact that some re/insurers reported that they are working to improve their cyber pricing models (e.g. by creating or purchasing databases from external providers).[6]

Fundamental Concepts : Cyber-attacks fall into a broader context than what is traditionally called information operations. Information operations integrated use of the main capabilities of electronic warfare, psychological, computer network, military trickery and security operations in coordination with special support and relevant abilities and to penetration, stop, destroy or hijack human decisions and it is one of the decision-making processes of national institutions. Fig. 1 describes the anatomy of a cyber-attack. From the USNM Strategy for cyberspace operations, computer network operation is composed of the attack, defense, and utilization enabling. The latter is different from network attacks and network defense, because this type of operation focuses more on collection and analyzing information than interrupting networks, and may itself be the prelude to an attack. These operations can be carried out of disseminating information and propaganda purposes. Computer network exploitation enabling operations can also be carried out with the aim of stealing important computers data. In such a context, Trap Sniffers and Doors are beneficial tools for cyber espial. Trap Doors permit an external user to accessibility software at any time without the knowledge of the computer user. Sniffers are a tool to steal usernames and passwords. The consequences of cyber warfare can include the following :

- The overthrow of the system of government or the catastrophic threat to national security; a simultaneous initiation of physical warfare or groundwork and facilitate the start of physical warfare in the near future;
- Catastrophic destruction or damage to the political and economic relations of the country;
- Extensive human casualties or danger to public health and safety;
- Internal chaos;
- Widespread disruption in the administration of the country;
- Destroying public confidence or religious, national and ethnic beliefs;
- Severe damage to the national economy;
- Extensive destruction or disruption of the performance of national cyber assets.

In addition, five scenarios can be considered for cyber warfare: (1) Government-sponsored cyber espionage to gather information to plan future cyber-attacks, (2) a cyber-attack aimed at laying the groundwork for any unrest and popular uprising, (3) Cyber-attack aimed at disabling equipment and facilitating physical aggression, (4) Cyber-attack as a complement to physical aggression, and (5) Cyber-attack with the aim of widespread destruction or disruption as the ultimate goal (cyber warfare). One type of cyber-attack is encryption. Encryption is a reversible method of encrypting data that requires a key to decrypt. Encryption can be used in conjunction with encryption, which provides another level of confidentiality. Encryption is the implementation and study of data encryption and decryption thus that it can only be decrypted by specific individuals. The system for encrypting and decrypting data is the encryption system. Encryption is a powerful tool for protecting important and private information when exposed to threats from strangers and criminals, as well as for hiding unauthorized activities from law enforcement. As computers grow faster and failure methods become more secure, cryptographic algorithms require sustained consolidation to prevent insecurity. Note that, in general, a distinction can be made between cyber-crime, cyber-warfare, and cyber-attacks. [5]

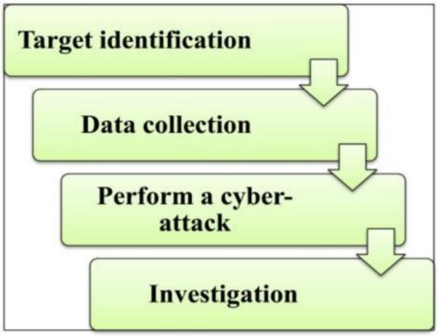

Fig: Anatomy of a cyber- attack

Cyber Security: Privacy and security of the data will always be top security measures that any organization takes care. We are presently living in a world where all the information is maintained in a digital or a cyber form. Social networking sites provide a space where users feel safe as they interact with friends and family. In the case of home users, cyber-criminals would continue to target social media sites to steal personal data. Not only social networking but also during bank transactions a person must take all the required security measures.

Incidents	Jan-June 2012	Jan-June 2013	% Increase/Decrease
Fraud	2439	2490	2
Intrusion	2203	1726	(22)
Spam	291	614	111
Malicious Code	353	442	25
Cyber Harassment	173	233	35
Content related	10	42	320
Intrusion Attempts	55	24	(56)
Denial of Services	12	10	(17)
Vulnerability Reports	45	11	(76)
Total	5581	5592	

The above Comparison of Cyber Security Incidents reported to Cyber999 in Malaysia from January–June 2012 and 2013 clearly exhibits the cyber security threats. As crime is increasing even the security measures are also increasing. According to the survey of U.S technology and healthcare executives nationwide, Silicon Valley Bank found that companies believe cyber-attacks are a serious threat to both their data and their business continuity.

- 98% of companies are maintaining or increasing their cyber security resources and of those, half are increasing resources devoted to online attacks this year
- The majority of companies are preparing for when, not if, cyber attacks occur
- Only one-third are completely confident in the security of their information and even less confident about the security measures of their business partners.

There will be new attacks on Android operating system based devices, but it will not be on massive scale. The fact tablets share the same operating system as smart phones means they will be soon targeted by the same malware as those platforms. The number of malware specimens for Macs would continue to grow, though much less than in the case of PCs. Windows 8 will allow users to develop applications for virtually any device (PCs, Tablets and smart phones) running Windows 8, so it will be possible to develop malicious applications like those for Android, hence these are some of the predicted trends in cyber security.[3]

Goals : The majority of the business operations run on the internet exposing their data and resources to various cyber threats. Since the data and system resources are the pillars upon which the organization operates, it drives lacking maxim that a risk to these individuals is definitely a threat to the group itself. A threat can be anywhere between a minor bug in a code to a complex cloud hijacking liability. Risk assessment and estimation of the cost of reconstruction help the organization to stay prepared and to look ahead for potential losses. Thus, knowing and formulating the objectives of cybersecurity exact to every organization is crucial in protecting the valuable data. Cybersecurity is a practice formulated for the safeguard of complex data on the internet and on devices safeguarding them from attack, destruction, or unauthorized access. The goal of cybersecurity is to ensure a risk-free and secure environment for keeping the data, network and devices guarded against cyber terrorisation.

Goals of Cyber Security?

The definitive objective of cybersecurity is to defend the data from actuality stolen or co-operated. To attain this, we aspect at 3 important goals of cybersecurity.

1. Defensive the Privacy of Information
2. Conserving the Integrity of Information
3. Controlling the Obtainability of information only

To approved users these objectives practise the confidentiality, integrity, availability (CIA) triad, the base of entirely safety agendas. This CIA triad model is a safety model that is intended to guide strategies for data security inside the places of a society or corporation. This model is similarly mentioned to in place of the AIC (Availability, Integrity, and Confidentiality) triad to side-step the mistake with the Central Intelligence Agency. The rudiments of the triad are reflected the three greatest vital mechanisms of safety. The CIA standards are one that greatest of the societies and businesses practice once they have connected a new request, makes a record or when assuring access to approximately information. On behalf of data to be totally safe, all of these safe keeping areas must originate into result. These are safe keeping strategies that all effort together, and hence it can be incorrect to supervise one policy.

CIA triad is the greatest collective standard to measure, choice and appliance the proper safety panels to condense risk.

Confidentiality : Making guaranteed that your complex satistics is reachable to accredited users and safeguarding no informations is revealed to unintended ones. In case, your key is private and will not be shared who power adventure it which ultimately hampers Confidentiality.

Methods to safeguard Confidentiality:

- Data encryption

- Two or Multifactor verification
- Confirming Biometrics

Integrity: Make sure all your data is precise; dependable and it must not be changed in the show from one fact to another.

Integrity ensure methods:

- No illegal shall have entrance to delete the records, which breaks privacy also. So, there shall be
- Operator Contact Controls.
- Appropriate backups need to be obtainable to return proximately.
- Version supervisory must be nearby to check the log who has changed.

Availability : Every time the operator has demanded a resource for a portion of statistics there shall not be any bout notices like as Denial of Service (DoS). Entirely the evidence has to be obtainable. For Example, a website is in the hands of attacker's resultant in the DoS so there hampers the obtainability.

Here are few steps to maintain these goals :

1. Categorising the possessions based on their position and precedence. The most important ones are kept back safe at all periods.
2. Holding down possible threats.
3. Determining the method of security guards for each threat
4. Monitoring any breaching activities and managing data at rest and data in motion.
5. Iterative maintenance and responding to any issues involved.
6. Updating policies to handle risk, based on the previous assessments.[2]

Cyber Security Techniques:

1. Access control and password security : The concept of user name and password has been fundamental way of protecting our information. This may be one of the first measures regarding cyber security.

2. Authentication of data : The documents that we receive must always be authenticated be before downloading that is it should be checked if it has originated from a trusted and a reliable source and that they are not altered. Authenticating of these documents is usually done by the antivirus software present in the devices. Thus a good antivirus software is also essential to protect the devices from viruses.

3.Malware scanners : This is software that usually scans all the files and documents present in the system for malicious code or harmful viruses. Viruses, worms, and Trojan horses are examples of malicious software that are often grouped together and referred to as malware.

4.Firewalls : A firewall is a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet. All messages entering or leaving the internet pass through the firewall present, which examines each message and blocks those that do not meet the specified security criteria. Hence firewalls play an important role in detecting the malware.

5. Anti-virus software: Antivirus software is a computer program that detects, prevents, and takes action to disarm or remove malicious software programs, such as viruses and worms. Most antivirus programs include an auto-update feature that enables the program to download profiles of new viruses so that it can check for the new viruses as soon as they are discovered. An antivirus software is a must and basic necessity for every system. [3]

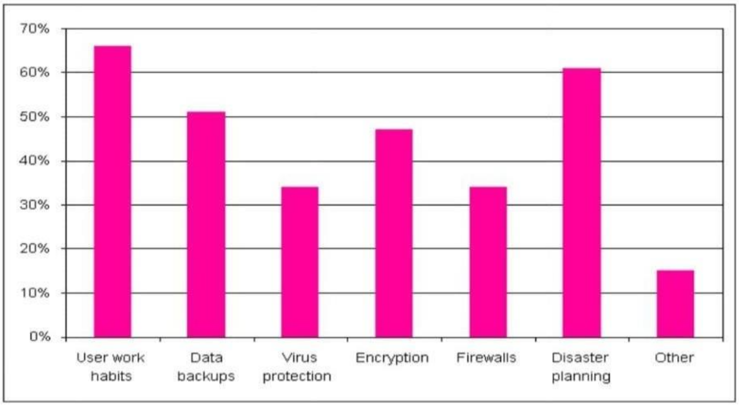

TABLE: Technique on cyber security

Methodlogy: The methodology adopted followed a systematic literature review (SLR), proposed by authors in, to derive conclusions and reflections about the above research questions. This academic approach helped us gather, examine, sort, and study the pertinent papers within the topic frame. The recommended guidelines of this method consist of three main stages:

- Planning the review, which focuses first on the identification of the need for a review, their proposal, and the development of their protocol;
- Conducting the review involves identifying the research using predefined keywords and search strings, selecting the studies based on inclusion and exclusion criteria, performing a study quality assessment using predefined criteria and checklists, extracting data, and monitoring progress before summarizing findings and providing data synthesis;

- Reporting recommendations and disseminating evidence through a descriptive analysis of findings and insights.

Consulting several reputable academic libraries helped us to gather pertinent articles related to our subject and respond to the research questions. These libraries are as follows:

1. ACM (Association for Computing Machinery) digital library;
2. JSTOR;
3. IEEE Xplore digital library;
4. MDPI;
5. Science Direct;
6. Scopus;
7. Springer;
8. Web of Science.

The current study aims to collect pertinent papers published from 2016 to 2024. To this end, many specific keywords are used in the research methodology during this period, such as: —CPE and CVE‖, —vulnerability detection‖, —vulnerability assessment‖, —CWE and vulnerabilities‖, —matching vulnerabilities‖, —asset inventory and CPE‖, —vulnerability detection and AI‖, —CVE and CPE by graph‖, —CVE and CPE by FM‖ and —VMS and vulnerability detection‖.

As shown below in Figures 1 and 2, the research method consisted of four procedures to gather the most significant papers related to our subject. The first stage involves gathering and building a global overview of the scientific contributions found in the literature review. Next, this study initially retrieved 846 papers from the academic libraries. By eliminating duplicates and out-of-scope papers, and classifying the publications using the abstract and title, the paper number was reduced to 487 papers. Then, 256 articles were selected by using predetermined criteria relevant to our topic. The following criteria were adopted:

- Papers published within the last 8 years;
- Relevant papers according to the research question posed previously;
- Papers suggesting vulnerability detection methods;
- Methods leveraging the usage of basic security metadata or AI techniques;
- Papers offering well-documented research on the proposed methods.

To provide unbiased research, the analysis was limited to academic contributions focusing on the described methods relative to our topic. Ultimately, data analysis results(125 articles) were separated into two studies: the main study, which conducts a thorough and deep investigation of the article‗s content, and the connected study, which is sufficiently investigated to derive further insights and future contributions.[4]

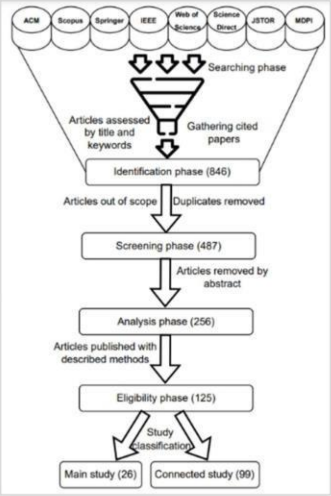

Fig 1: Process of the methodology used in the literature

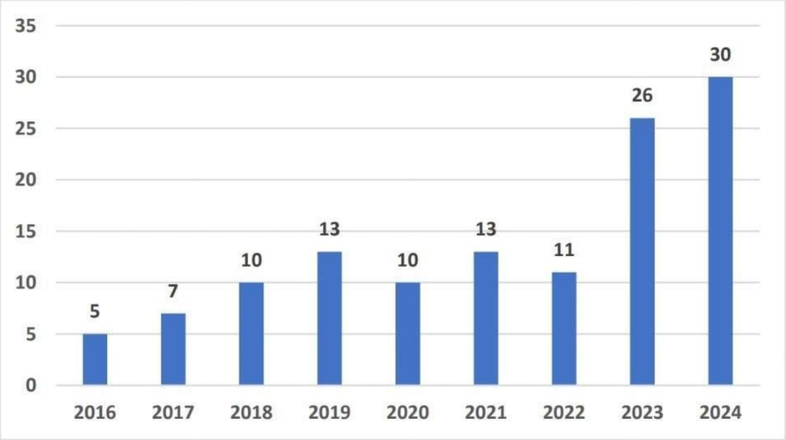

Fig 2: Distribution by year of the analysis study

Conclusion : Computer security is a vast topic that is becoming more important because the world is becoming highly interconnected, with networks being used to carry out critical transactions. Cyber-crime continues to diverge down different paths with each New Year that passes and so does the security of the information. The latest and disruptive technologies, along with the new cyber tools and threats that come to light each day, are challenging organizations with not only how they secure their infrastructure, but how they require new platforms and intelligence to do so. There is no perfect solution for cyber crimes but we should try our level best to minimize them in order to have a safe and secure future in cyber space.[3]

References:

1. Valuing the cyber-attacks budget in high voltage power substations to increase cyber-security; providing a method based on Fuzzy Analytical Hierarchy Process - Yongcai Xiao, Lianghan Yang, Jun Li, Jian Xu, Kuangye Liu
2. Researh paper on cyber security-Mrs. Ashwini Sheth, Mr. Sachin Bhosale, Mr. Farish Kurupkar
3. A study of cyber security challenges and its emerging trends on latest technologies -G.Nikhita Reddy, G.J.UGANDER Reddy
4. A comprehensive review and assessment of cybersecurity vulnerability detection methodologies- Khalid Bennouk, Nawal Ait Aali, Younès El Bouzekri El Idrissi , Bechir Sebai, Abou Zakaria Faroukhi and Dorra Mahouachi

❑❑❑