AN INVESTIGATION AND ANALYSIS OF CYBER SECURITY INFORMATION SYSTEMS: LATEST TRENDS AND FUTURE SUGGESTION

Tarun Dhar Diwan[1], Dr. Siddartha Choubey[2],Dr. H.S. Hota[3]

[1] *Chhattisgarh Swami Vivekanand, Technical, University, Bhilai, Chhattisgarh, India*

[2] *Shri Shankaracharya Technical Campus, Bhilai, Chhattisgarh, India*

[3]*Atal Bihari Vajpayee University, Bhilai, Chhattisgarh, India*

Abstract: Network protection includes of the strategies and procedures implemented in this paper to avoid and monitor intrusion attempts, infringement, manipulation or violation of a computer system and services accessed by the network. Network protection applies to the different countermeasures put in place to secure or flow through the network and data collected on or through it. Protection for web applications is the method of securing websites and internet resources from multiple security attacks that target weaknesses in an application. Security for web apps is a data management division that primarily deals with the security of websites, web applications and web services. Risks to cyber security include a broad range of allegedly criminal practices on the web. For years, computer security risks against utility assets were identified, cyber-attacks arising from the exploitation of data device weaknesses by unauthorized access users This study is a cyber infrastructure assault, vulnerability and vulnerabilities, including hardware and software devices, networks, business networks, intranets, and cyber intrusion usage. Only big organisations are at risk of cyber-attacks, a widespread misunderstanding. Even then, the targeting of small and medium sized enterprises has seen a large improvement. This is since less-sophisticated cyber defence mechanisms appear to be used by these smaller organisations. As many as 50% of all cyber-attacks hit small companies, wasting $200,000 on average, sufficient to get out of business for less-established entities. an enterprise-grade protection device and awareness of the various forms of cyber threats facing corporations in 2025 to safeguard company from hacking attacks. fight cyber threats successfully and decrease the exposure of enterprise.

Keywords: Unauthorized Access; Internet; Intrusion; Security; Cyber Infrastructure; Attack; Machine; Vulnerabilities; Threats.

Introduction

A machine literate person is the most powerful defence in cyber security accidents involving threats, study confirms. The most susceptible to remember are those described on this analysis like fresh hires inside organisation, especially among intruder requesting private identifying information from individuals concerned [1]. The psychological factors that lead to the insecurity of users and networks are further supported in this review. This research suggests that whereas innovation has a huge part to play in mitigating the effect of hacking, human actions, human desires and psychological behavioural patterns that can be impacted by education remain challenged and fragile [2].It is possible to reduce hacking attacks, but an ultimate approach for addressing certain cyber security issues is still yet to be put forward. Cyber security is a diverse issue that needs skills and experience from a wide variety of fields, including, though not bounded to, information technology and computer science, engineering, organisational performance, economy, psychology, political science, sociology, decision-making, global affairs, & legal-process [3]. While analytical steps are an essential aspect, cyber protection is not solely a technical issue, although it is possible to get lost in technical information for policy experts and many others. In comparison, what is understood about cyber security is frequently compartmented into disciplinary lines, limiting the cross-fertilization perspectives available[4].

A cyber-attack is an organized action to manipulate technology-dependent networks, computer systems, and organizations. To alter computer files, coding, or logic, cyber-attacks use malicious code, sometimes resulting in data breach and often identity or knowledge stealing[5]. A computer network attack, or CNA, is also considered a cyber-attack. When enterprise technologies and security systems continue developing, cyber attackers employ tactics as well.Corporations have lost $2.7 billion globally due to cybercrime, and analysis suggests that this figure will continue to rise annually [6]. Ransoms charged to cyber criminals, fines, funds paid for upgrades and maintenance, and the

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

expenses involved with missing customers and reduced credibility are counted in these damages [7].

(a) Cyber-Attacks: In the internet world, cyber-attacks are a major concern which must be concentrated on due to the effects upon resources and records that is highly sensitive. Technologies advancement followed by cyber security risks either "cyber-attacks" that endanger the protection of consumers while using those technologies. It is hard to detect and avoid cyber vulnerabilities and assaults[8].

(b) Untargeted attacks: Un-targeted threats have indiscriminately targeted perpetrators as potential customers and utilities. They uncover the vulnerabilities of the network or utility. Phishing: Phishing involves bogus individuals sending emails to numbers of users and asking for personal details such as baking, credit card. Attackers may take advantage of technology such as: They promote false website visits and send nice deals. To enter their records, the customers click on the email links, and so they remain unaware that the fraud has occurred. [8], Water holing: release the bogus website and even the dummy website or hack a real one to manipulate the details of the user browsing. Ransom ware: Contains spread disk encrypting ransomware for extorting. Scanning: Arbitrarily targeting vast swaths of the Internet [9].

(c) Targeted attacks: targeted attacks on attackers, targeted attacks on cyber-based consumers. Spear-phishing Sending malicious software and promotional links via emails to targeted individuals that could contain malicious software for downloads [10]. Botnet implementation. It offers a distributed denial of service (DDOS) attack that subverts the supply chain. To target the network or applications distributed to the enterprise in general, attackers can use tools and techniques to test the networks for an exploitative flaw in the first place [11].

(d) Vulnerability: They are flaws for the system or its architecture which cause instructions to be executed by an attacker, unapproved data to be accessed, and/or service denial attacks to be carried out [12]. Vulnerabilities can be found in a number of applications in different fields. Vulnerabilities in the hardware or applications of the system, vulnerabilities in the policies and processes employed in the programs and deficiencies of the users of the system themselves may be concerned [13]. Due to equipment usability and interoperability, weakness has been recognised and even the effort required to repair it. Computer bugs, such as communication protocols and disk drives, may be contained in operating systems, application software, and control system[14].

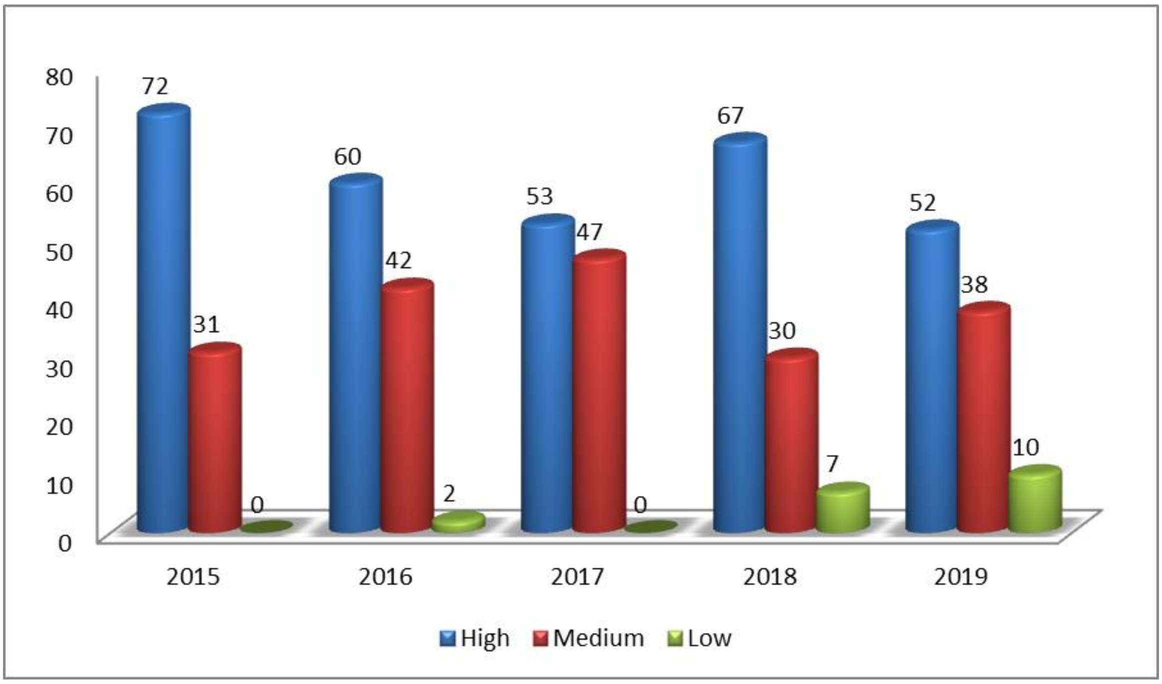


Figure 1: Maximum Severity of Vulnerabilities Found in Websites

Software design errors are caused by a range of causes, along with human factors and applications complication [15]. Human errors are typically the root of technological vulnerabilities. [16] No device is resistant to cyber attacks by nature, and the effects of avoiding the dangers of complacency, ignorance, and incompetence are evident. Zero-day attacks have been found in an unparalleled amount of bugs, and web assault exploit kits are adapting and improving them quicker than ever. Vulnerabilities can be abused as more computers become connected. [17].

I. CLASSIFICATION OF CYBERATTACKS

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

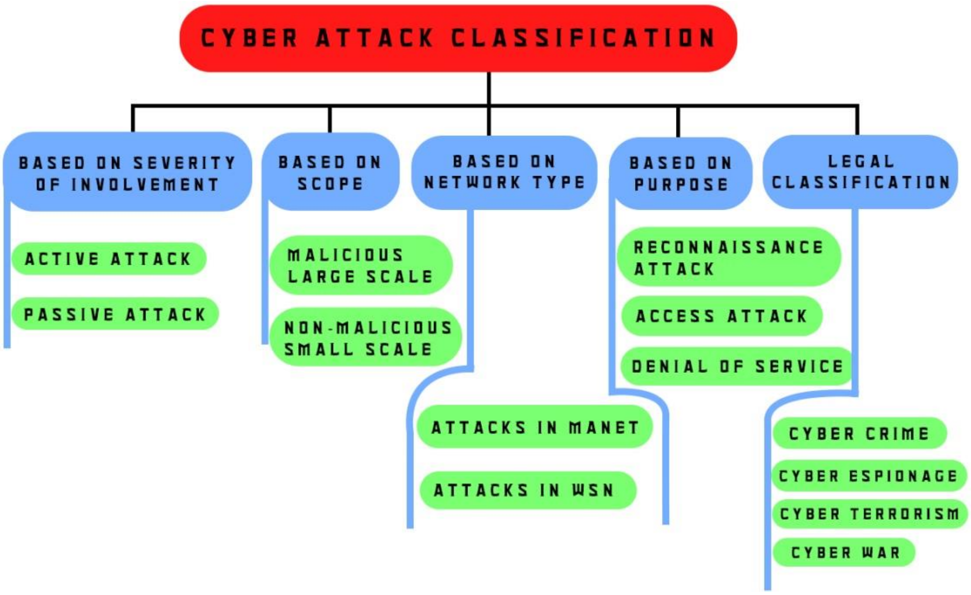


Figure 2: Cyber Attack Classification

1. **BASED ON SEVERITY OF INVOLVEMENT**

Strikes could possibly be categorized depending on intensity and interest on the offense. In two pieces, Passive and Active Attacks may be studied.

i. Passive Attack: In order to play the data contained in a device by call hearing, or the intruder is passively listening to the conversation between both the two parties [18]. In comparison, dissimilar from active attack, the DB may not be opened, but a violation could also have been attempted [19].

ii. Active Attacks: cause by the intruder to unidirectionally / bidirectionally transfer packets to other or obstruct data transfer [20]. An analysis of Cyber Terror Passive Attacks Research Studies.

2. **BASED ON SCOPE**

i. Also group cyber-attacks as per their area of interest. There are: Non-Malicious Small Scale and Malicious Big Range [21].

ii. Suspicious Wide Scale The purpose of attackers in this category is to achieve personal or group advantages or compromise the efficiency of the system. Attacks that interrupt the goal device or cause disruption in society include certain Attacks that interrupt the goal device or cause disruption in society include certain [22].

iii. Non-Malicious Small Scale These are threats which harm little part of the objective infrastructure, lead minimum harm to property, or lead loss of data that will be recoverable. It is carried out by inexperienced attackers or staff of novices [23].

3. **BASED ON NETWORK TYPE**

Attacks on types of networks are categorised as Mobile Adhoc Networks (MANET) and Wireless Sensor Networks (WSN).

i. **Attacks in MANET** In this range, there are several attacks, including: Byzantine Assault, Black Hole Attack, Flood Rushing Research Studies [24].

ii. **Attacks on WSN** in this type, there are two attacks. There are: Network Layers-based attacks and attacks related to cryptography and non-cryptography [25]. With the regional aspect of certain cyber-attacks, along with global security concerns, methodological and ideological strategies are discussed. During this stage, data and studies on cyber security show a conceptual pattern about the growth of cyber terror [26]. Enhanced cyber space dependency generates distinct scores in the terror dimension. A cyber warfare phenomenon is generated by this classification of cyber-attack and terrorism [27].

4. **BASED ON PURPOSE**

If the attacks are subdivided as per their goals, Reconnaissance, Access and Denial of Service attacks appear.

i. **Reconnaissance Attack** System mapping experiments was included in the results for unauthorized areas and resources. Packet sniffing and port scanning attacks are examples of reconnaissance attacks.[28]

ii. **Access Attack** An attacker with no access rights can exploit a flaw in the system or penetrate it to obtain data. Man-in-the-middle attacks, social engineering, and phishing are all examples of this type of attack. [29].

iii. **DoS** referred to machine being slowed down or machine being interrupted. With this, it is also possible to corrupt or erase records [30].

5. **LEGAL CLASSIFICATION**

In this community, there's cyber terror. The sub-groups for cyber-attack legal classifications is: Cyber Bullying, International Conflict, Cyber Crime, Cyber Terror,Cyber Warfare and

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

Civil War [31]. War of Information can be defined as conducting the operation which would have an effect on other side's information systems, information-based processors and information-based network systems and defending their own systems [32]. It is intended to encourage repeated aggressive behaviour or to damage others personally or as a group.It is done by the usage of ICT(information and communication technology), like , the use of smart phone software, instant message apps or the posting of humiliating websites [33].

i. **Cyber Crime** It can be described also as "use of IT to encourage the handling of unlawful behaviour or offences." The term computer crime applies to any offences including, in the broadest sense, the use of IT. Malwares, logical bombs, worms are examples of this category. Electronic criminals, cybercrime, IT crime, high-tech crimes, and web-based crimes are also used mutually. 184 A study of Cyber Terror Research Reports [34].

ii. **Cyber Espionage or Cyber Spying** This community contains venerable programs ex: Trojan horses and spyware, as well as target device capture approaches. The unlawful usage of tools or techniques & the collection of valuable information from unsanctioned or classified locations is cyber theft or surveillance. Specifically, professional spies, malicious intruders or coaders may execute such exercises [35].

iii. **Cyber Terror** Cyber terror is just another type of worry that has developed over time and mutated in the twenty-first century. Terrorist attacks like these are easy to be carried out, and the damage they cause is unfathomable. It's just a feeling of anxiety against which it is very difficult to combat. Cyber terror, according to the FBI definition, is an event that can lead to anarchy by damaging the operation of organizations and vital infrastructure [36].

iv. **Cyber War or Cyber Warfare** This definition of cyber warfare can be described as a state's intrusion operations carried out to harm or suspend another state's computer systems or networks [37].

6. **Cyber Security Vulnerabilities**There are a few flaws in cyber security that are exploited more frequently by attackers [38]. A list of the top 5 cyper security flaws that have inflicted the greatest damage to companies this ten years can be found below:

- Substandard back-up and repair
- Poor management of authentication
- Inadequate control of the network
- Mistakes and/or abuse by end-users
- Poor protection at the end-point

II. TYPES OF CYBERATTACKS

Cyber Défense covers several forms of threats. And while threats are changing every day, Cybercriminals rarely try to create something new. Rather, they depend heavily on methods that have proven to be effective in the past[39]. The following list of cyber threat types concentrates on the ones that hackers use most often. included equipment recommendations for each category to aid in business protection. I'll go over these methods in greater detail in the second quarter of this post [40].

1. **SQL Injection Attack**

A usual concern for database-driven websites has been the SQL injection attack. These attacks happen when a cybercriminal performs a query and issues it to a database, transmitted by the input data from the client to the server [41]. The SQL query is inserted, often instead of the passwords or login credentials, into the data-plane entry [42]. This makes it possible for cybercriminals to execute their own predefined SQL orders. Critical information may be read, stolen, changed, added, altered, or removed when a SQL - injection attack is accomplished [43]. Cyber criminals can even perform maintenance procedures on the database, such as shutdown; retrieve material from any given file; and even send commands to the OS.

SQL injection detection tools:

- SolarWinds SEM
- ManageEngine EventLog Analyzer

2. **Phishing and Spear Phishing Attacks**

A phishing attack requires the posting of emails by cybercriminals that claim to be from reputable sources. The purpose of this type of attack is to extract confidential information from an individual or to manipulate them to be doing something [44]. For example, it may feature an addon that, when opened, installs malware onto the computer. Optionally, to force somebody to hand over their data or trick them into installing malicious programs, it could include a connection to a bogus website [45].

There is more targeted spear phishing. In order to create a personalized and personal email, these attacks enable the attackers to perform analysis into their targets. It makes spear spoofing very hard to protect toward. The "from" field of an email, for example, may be false, prompting the receiver to assume that the letter is from someone they know; or an email could appear to be from the employer of an individual, asking for immediate funds. Cloning a legitimate website is another common spear phishing tactic, thereby tricking an individual to enter their login information or personally identifiable information [46].

Spear Phishing detection tools:

- SolarWinds SEM
- SolarWinds IM

3. **Malware.**

Malware is unwanted software that runs on a machine or computer without the user's prior consent. Malicious software also

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

penetrate the computer by adding and propagating genuine script to it [12]. It can conceal or repeat itself through the Internet in apps [13]. many various types of viruses are there, and new ones emerge every year, but the following are most common types of malicious software:

- **Macro Viruses :** By adding themselves to their initialization process, small malicious contaminate programs, such as Ms Word & Excel. The macro virus executes commands as the program starts up and passes access to the infected program [15]. Then it reproduces another code and adds it to it.
- Trojans: mischievous software hidden within trusted software, often referred to as a trojan horse. Trojans can't reproduce the distinction between regular viruses and Trojans. they as well build side way for potential assaults be used. A trojan, for instance, may be built to construct a high-numbered port, enabling a new attack to be executed by the intruder [23].
- **Stealth Viruses:** By taking charge of system operations and systems, these viruses hide themselves. They bypass tools for malware identification, so contaminated parts of the device are recorded as uninfected. Stealth viruses are able to mask an improvement on the volume of the directory manipulated & modifications upto last update time of the file [29].
- **Logic Bombs:** one more instance venerable s/w is Logic Rockets. Such bombs bind themselves to an application and, such as a certain time or date, are caused by particular events.
- **Ransom ware:** Ransom ware is a form of virus which prevents users from accessing data on their devices. When the ransom is not paid, the intruder will even threaten to publish or erase confidential material [36]. Simple ransom ware is pretty easy to patch, but it is almost difficult to retrieve the data when an attacker uses more complex ransomware such as crypto viral blackmail [37].
- **Adware:** As part of their marketing campaigns, Adware is a software application used by corporations. It generally occurs as ads or banners viewed when apps are running. Bloatware will instantly update itself to computer when visit a site [36].
- **Spyware:** This form of cyber-attack is intended to gather the victim's data, particularly their surfing habits. Excluding permission or awareness, Spyware monitors anything and sends the details straight to inaccessible person [41]. It will set up other venerable programs through the web on device.

Malware detection tools:

- Malwarebytes
- SolarWinds SEM
- SolarWinds Patch Manager

4. Botnets

It includes micro-computers or machines operating together accomplish single mission. name that "botnet" since systems exist through a network of computers, otherwise known as bots, or robots [39].

Solo bot may not make that major harm, strong & probably unsafe collectively. Malicious hackers are using botnets to drive a number of cyber threats. For example, they may assist a cyber attacker to encourage DoS Attack that website among public load intended to render it disconnected [13]. This assault will charge a corporation loss of millions of $, consumers. This are sometimes applied to rob, transmit spam, & scatter viruses from passwords & personal information. since they cheap and powerful, are common tools for cybercriminals. employ a robust IT protection solution to defend organization from botnets [32].

A bot assault can be used to circumvent security mechanisms for corporate firewalls and may theoretically computers, converting bot node. Unless they create contact, these bots will remain benign [28]. A variety of attacks can then be performed by Bot squads many.

Botnet detection tool:

● SolarWinds SEM

5. Cross-Site Scripting Attacks

In an individual's scripting software or web browser, Xss, also known as cross-site scripting attacks, use third-party online tools to enforce codes. An intruder loading a payload infected with malicious JavaScript into a webpage database is an example of an XSS attack [31]. If the intended victim wants to go to a specific page on this website, that page is not available. sent as part of the HTML body with the payload. It is then communicated to the browser of the intended victim, which triggers the script [39].

The js coding might submit victim’s cookie to the server of the Intruder. that will enable hackers to retrieve & then use that for purposes of session hijacking. If used to manipulate other vulnerabilities, XSS may have serious repercussions, and might theoretically allow the intruder to take snapshort, monitor keyboard operation, thieve network record, and still access the accused's computer remotely. use ActiveX, Flash, VBScript, and JavaScript to start an attack. Although JavaScript is universally embraced, it is the most frequently abused Cross site scripting attack execution process [26].

Many web apps have flaws that allow cyber attackers to distort the website they are visiting. All the intruder needs to do to snag a target is make it to connect among those unauthorized web pages also press on the mischievous codes unknowingly [16]. Considering in what way quickly anyone may decrease prey to an attack of this sort, it

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

is of vital significance to use an appropriate defence approach.

Cross-site scripting detection tool:

- SolarWinds SEM

6. DENIAL OF SERVICE AND DISTRIBUTED DENIALOFSERVICE ATTACKS

Hackers use DoS attack to exhaust the infrastructure of a system, which enable the user to become non - responsive to service calls. The system's assets are often attacked by DDoS attack, but the root of the release comes from a vast variety of host computers, each compromised and under the control of the cyber attacker [25]. In collaboration with botnets, DDoS attacks operate and are proficient of totally crippling a webpage or e-services. By overtaking the objective along torrent of action from lots and even huge amount of gadgets in a botnet, they do this [32].

DoS attacks do not explicitly support the person responsible for the attack, unlike other attacks that are typically targeted at helping the attacker to obtain entry. Cyber criminals appear to be content with sheer denial of service in some situations. If, however, a rival company controls the desired resource, DoS attacks may favour the intruder by ruining the prestige and ability of their opponent to provide services. Another explanation why DoS or DDoS may be used by an attacker is to make the machine vulnerable to another attack. A cyber intruder might any benefit, by taking the device offline [21].

There are so many flood attacks by

- **TCP SYN Flood Attacks:** The cyber intruder utilizes the data buffer area at the time of initially set handshake of a TCP session to accomplish a TCP SYN flood assault. Attacker will flood in-process queue of the victim's device with a mass of link requests by abusing the buffer space, but does not respond to request responses. The machine times out as a result, and flood on link sequence make them to fail. By positioning host bottom a barrier designed to block SYN packets and through increasingly link queue size while decreasing the timeout on live connections, from TCP SYN flood attack [8].
- **Smurf Attacks:** In order to overload the user's network with traffic, It include using the ICMP and IP spoofing. This method of attack uses ICMP echo demands, which come from a false address for the victim. Unless the targeted IP address was 10.0.0.10, for example, then the cyber attacker will produce a bogus ICMP echo appeal within the matching address no. and deliver the demand to the 10.255.255.255 broadcast address [5]. It would then submit this ICMP request to all the IPs in the set, but all replies would be forwarded to the addresses of the purpose. This overwhelms the network, in essence. It is possible to replicate and even simulate smurf attacks, leading in significant data traffic [28]. need to incapacitate router's IP- guided publishes to shield from smurf attacks. Alternatively, customize the end systems to prohibit ICMP packets emanating from broadcast addresses from reacting to them [15].
- **Ping of Death Attacks:** The death threat ping pings the device of a target for anyone IP size larger than the immense amount of bytes. To do this, it utilizes IP packets. After all, Data packet of such length was n't permissible, so the cyber attacker has to break the IP packet. once that users machine rebuilds the packet, crashes are eventually encountered [22]. Using a powerful firewall to search for maximum length for broken IP packets will avoid these kinds of attack.
- **Teardrop Attacks:** this allows the sequential IP packets' size & splitting offset fields to interfere with each other on the intended host. The focused machine attempts to rebuild the packets with little luck during this process, and the system crashes under pressure [18]. To defend them against this form of DoS attack, it's essential for users to have repairs.Be ensure uninstall SMBv2 and block ports 445 and 139 if don't have updates.

DDoS detection tools:

- PfSense
- SolarWinds SEM

IV. CYBER SECURITY THREATS

Threats A large spectrum of potentially criminal internet practices are protected by cyber security threats. For decades, cyber security risks against utility infrastructure have been acknowledged. The acts of terrorism have therefore cantered attention on the defence of vital infrastructure. Insecure computer systems can lead to fatal interruptions, confidential information leakage, and theft. Cyber-attacks arise from the manipulation by users of unauthorized access to cyber device vulnerabilities[7].There are crimes specifically attacking networks or systems, like ransomware, viruses or DoS attacks and offenses aided by networks or computers, the main focus of which is fraud, identity stealing, phishing attacks, cyber stalking, irrespective of the network or system[27].

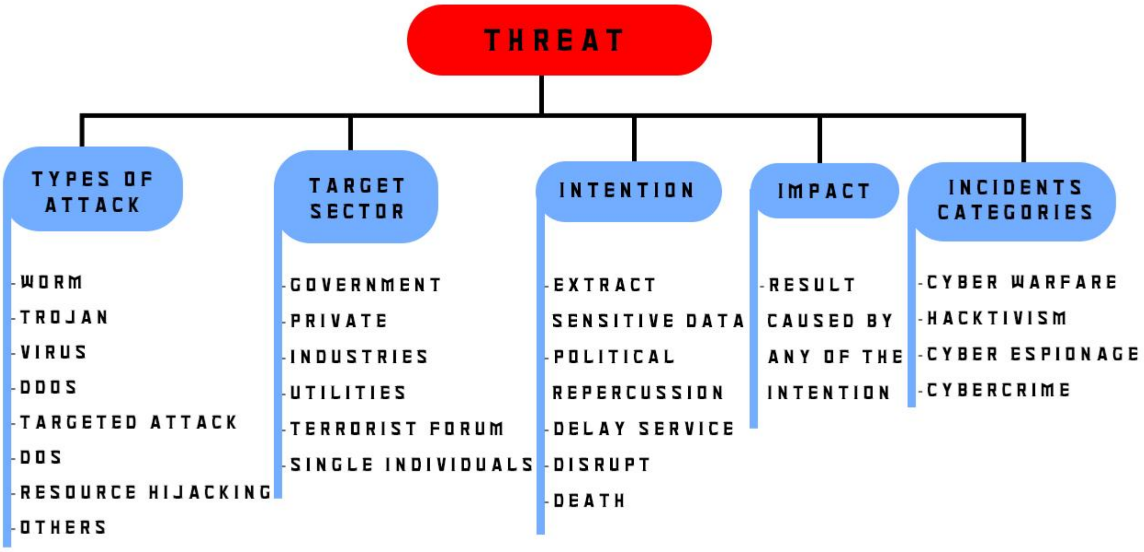


Figure:3 Classification of Threat

(a) TYPES OF ATTACK

- **Worms:** Worms diverge from viruses in that they do not connect to a host disc; instead, they are self-contained scripts that propagate across networks and computers. Worms are normally distributed via email attachments, with the worm programme being prompted when the connection is opened. In addition to fulfilling malicious activities, a typical worm bypass includes sending a copy of the worm to each connection in an affected computer's email account. A worm spreading throughout the web and loads email servers can result in DoS attacks targeting nodes. [35]. In its propagation worm, the attackers are like viruses with no guidance from the network.However, in worms, unlike viruses, no user input is required to cause their attempt to spread.
- **Trojans:** A Trojan, also known as a Trojan horse, is a malicious programme that sticks inside a useful programme. Trojans do not self-replicate, which is a significant distinction among viruses and Trojans. In order to generate assaults on a computer, a Trojan may build a back entrance that can be used by hackers. To begin, a Trojan are being encoded to open a heavy port, allowing an attacker to pay attention and then launch an attack. It is a malicious software that, even though the computer should be idle, creates unwanted changes to the computer environment and suspicious behaviour. This misleads the customer of its true meaning [17].
- **Virus:**It is a kind of malicious software application that is distributed without a user's awareness across the device files. It is a malicious self-replicating program that, when conducted, replicates by injecting copies of itself into other computer programs. Directions that inflict damage to the device may also be performed. The virus can be described as a piece of code that normally connects itself to another program, and this will run with them because the program is running [14].
- **Distributed Denial-of-Service (DDoS) Attack** A DDoS attack is often an attack on the infrastructure of the server, but it is launched from a vast number of other host devices compromised with attacker-controlled malicious programs. Apart from attacks which are meant to encourage the intruder to obtain or improve access, DoS attacks do not provide intruders with positive effects. It's enough to get the pleasure of service refusal for some of them. If the desired attribute, on the other hand, happens to a business competitor, the intruder's benefit could be accurate. Another aim of a DoS attack might be to take a device offline in order to initiate another kind of attack. Session hijacking[27]. There are various forms of DoS and DDoS attacks; TCP SYN flood attack, teardrop attack, smurf attack, ping-of-death attack, and botnets are the most common ones.
- **Target Attack:** A coordinated attack refers to a risk type in which threat actors deliberately pursue and damage the infrastructure of a target organization while preserving anonymity [31]. These attackers have a certain amount of experience and have ample leverage over a long-term duration to execute their schemes.To fight their victim's defence, they may adapt, modify, or intensify their attacks.
- **Denial of Service:** illustrates the orchestrated assaults on the functionality of the target machine service that has been delivered or a network initiated implicitly via a variety of corrupted computing devices [43]. It can be grouped into the following-

✓ DoS defeat the capacity of a device so that it does not replied for demands for service.

✓ It is an intrusion intended to make users inaccessible to a server or network resource. By flooding the target with traffic or giving it data that causes a crash, it does this. It uses a single device to target a computer and a single internet

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

connection [11].

- ✓ **Volume-based assaults:** The aim is to saturate the attacked site's bandwidth and is measured in bit per second.
- ✓ **Protocol attacks:** This uses the true resources of the server and is measured in a packet.
- ✓ **Application layer attacks:** The purpose is to crash the web server and per second is calculated in the submission.

- **Resource Hi Jacking There is a new "attack" running across the network. It is referred to as Resource Hijacking because it comes down to JavaScript that uses the computational resources to do stuff on behalf of the "intruder." In quotes, I use the term assault because it wasn't necessarily targeting, but just behaving without permission. One general aim of Resource Hijacking is to verify crypto-currency network transactions and gain virtual currency[46]. Adversaries can consume sufficient device resources to have a negative effect on affected machines and/or cause them to become non - responsive. Because of the high potential for usable services, servers and cloud-based platforms are common targets,**However, for resource hijacking and crypto currency mining, user endpoint devices can also be hacked and used [41].
- **Browser plugins:** Luckily, a few extensions to the browser will help preserve privacy and enhance online security. We propose a shortlist of browser extensions here:

(i). **HTTPS Everywhere:** opts for SSL-encrypted web page versions wherever accessible,

(ii). **Disconnect or Privacy Badger:** prohibits the use of monitoring cookies and related technology by websites to control activity online.

(iii). **Ad Block Plus:** ads are a prominent attack vector for users to distribute malware and phishing ads. They can be held at bay with a strong ad blocker.

(iv). **No Script or Script Safe:** Prevents the automatic running of JavaScript on server, stopping drive-by-downloads that can corrupt device with malware.

- **Theft:** it is greatest prevalent malware threat that has arisen in cyber world. it form of violation is generally mention to in the common perception as hacking. it means using the web to hack data or money [22]. It is calls unauthorized entry, without user knowledge or permission, to tamper with the sensitive data and by applying malicious code to smash or breach the operating device or network protection. Among others, it is the most serious cybercrime. This cyber-attack is the prey of several of the banks, Microsoft, Yahoo and Amazon. Tactics like plagiarism, malware, piracy, espionage, DNS cache poisoning, and self identification stealing are used by cyber thieves. Most of the websites for protection have being referred to several cyber risk [28].
- **Cyber Vandalism** Instead of stealing or misusing records, destroying or manipulating it is called cyber vandalism. It implies disrupting or stopping the effects on network networks. This deprives registered users of the information stored on the network from accessing it. This cyberterrorism is like a time bomb that can be set to take effect at a designated moment to destroy the target device [37]. Serious forms of cybercrimes are the development and distribution of dangerous software that causes irrecoverable harm to computer networks, intentionally injecting script such as viruses into a network to control, track, interrupt, avoid, or take some other operation without the consent of the network owner.
- **Web Jacking** Web lifting is the successful supervise over web based server by obtaining entry and regulate of another's website. The data on the web could be exploited by hackers [3].
- **Stealing payment records** Stealing credit or debit card information by stealing and misusing this information on the e-commerce server.
- **Cyber Terrorism** Deliberately, politically motivated violence against people is typically committed through the use of, or with the aid of, the internet. The National Academy of Sciences started a study on information security as early as 1990 with the words, "We are at risk." Increasingly, it relies on robots [8]. The terrorist of tomorrow could do more harm with a keyboard than with a keyboard
- **Child Pornography** develop, circulate, or view content which abuse underaged child pornographic in public clouds [15].
- **Cyber Contraband** The transmission over the internet of illicit products or content that is forbidden in other countries, such as restricted content.
- **Spam** This involves the violation of the SPAM Act by supplying unethical material marketing or unethical material proliferation through emails via unlawful transmission of spam [19].
- **Cyber Trespass** Legal access to network resources without altering data or system disturbances, abuse, or damage. It may include accessing personal information without distressing it or spying for some crucial data from the network traffic.
- **Logic bombs** There are services based on the case. These programs are triggered right after the signal of particular programs. The Chernobyl virus is a particular instance that functions like a rational bomb and will sleep at a specific date [21].
- **Drive by Download** Search engine corporations are conducting a survey. Website numbers have served as hosts for malware. Since its inception, word "Drive by Download " has been split into various variants in the

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

computing industry. This is remarkable development in some s/w application is computerized loaded when browsing on the internet on a consumer device [33]. The aim of setting-up mischievous programs is to obtain influence across the user computer, such as stealing sensitive information such as stored passwords, private details, using the user end as a botnet to distribute malicious content furthermore [17].

- **Cyber Assault by Threat** emails, videos or telephones, to intimidate an entity with fear of their lives or the lives of their families or others responsible for their safety (such as employees or communities). An instance of this is trying to blackmail an individual to a point where, via an internet banking facility, he is compelled to move money to an undetectable bank account [44].
- **Script Kiddies** Novices, also known as cyber criminals, script bunny, code kitty, and script running inexperienced [13], are people who use other people's passwords or programmes to target information systems, channels, achieve access permission, and vandalise sites.
- **Whist blower:** implies the leakage of knowledge inside the company for alleged misconduct, or the danger to persons or organizations who have the potential to take steps.
- **Account Hijacking:** It is characterized as a mechanism in which a specific computer, email, or other service-related account or computer system is hacked or theft by intruder [4].

(b) TARGET SECTOR

- **Government:** Buildings/housing, emergency care, necessary benefits, and welfare programs, state and federal governments, regional authorities, infrastructure, job safety, and atmosphere are also examples of municipal or central government [16].
- **Private:** refers to the portion of the organisation of a nation managed by individuals and corporations, rather than the state.
- **Industries:** industries composed of both machinery and installations used for the manufacturing, processing or assembly of goods [17].
- **Utilities:** The energy industry encompasses businesses such as manufacturers of power, water, coal, and integrated utilities [18].
- **Terrorism forum:** the target field for any terror organization.
- **Single Individuals:** This is the field in which the intruder tries to manipulate the individual consumers.

(c) INTENTION

- **Extract Data:** *Data extraction is a method that includes collection of different data sources. In order to process it further, enterprises often extract data, migrate the data to a data archive (such as a data warehouse or data lake) or further analyses it. As part of such a method, it's normal to convert the data [17].*
- ***Sensitive data:*** *Sensitive data is confidential material which, unless expressly allowed, must be shielded and which is unavailable to third parties. Data may be in tangible or electronic form, but confidential data is known to be private information or data in any case [24].*
- ***Political impacts:*** *refers to incidents that influence the government or the persons who lead the nation.*
- **Delay Service:** Because of the issues in the framework, organisations or firms miss delivering programs on schedule. Confidential data extraction: where unsanctioned individuals or intruder secure access to personal data and collect personal records [19].
- **Disrupt:** changing access, deleting data accessibility or access to a survivor. Exploit the authorization.
- **Other:** situations that do not come into any of the sections listed above.

(d) Impact: The effect of an event explains the result of the incident. Both impacted organizations, including information networks, the physical systems in which the cyber-physical environment communicates, and the wider impacts on the society and organisation, need to be discussed in the impact description[20].

(e) INCIDENT CATEGORIES

- **Cyberwarfare (CW):** "Use of cyberspace to attack personnel, facilities or equipment (by operating within or through it) in order to degrade, neutralize or destroy the enemy combat capabilities" [21].
- "**Hacktivism (H):** "is the fusion of the hacking process and advocacy in which hacking refers to operations that, typically with the aid of certain tools, manipulate computers in ways that are uncommon or even illegal" [22].
- **Cyber Espionage (CE):** an arm of high-tech organized corruption. This generally includes assaults on corporations and organisations and not people. Cyber espionage does not usually always take place on a broad scale [23].
- **Cyber Crime (CC):** The all-criminal act that deals with networks and machines includes (hacking). In addition, cybercrime involves typical crimes that are carried out through the Internet [24].

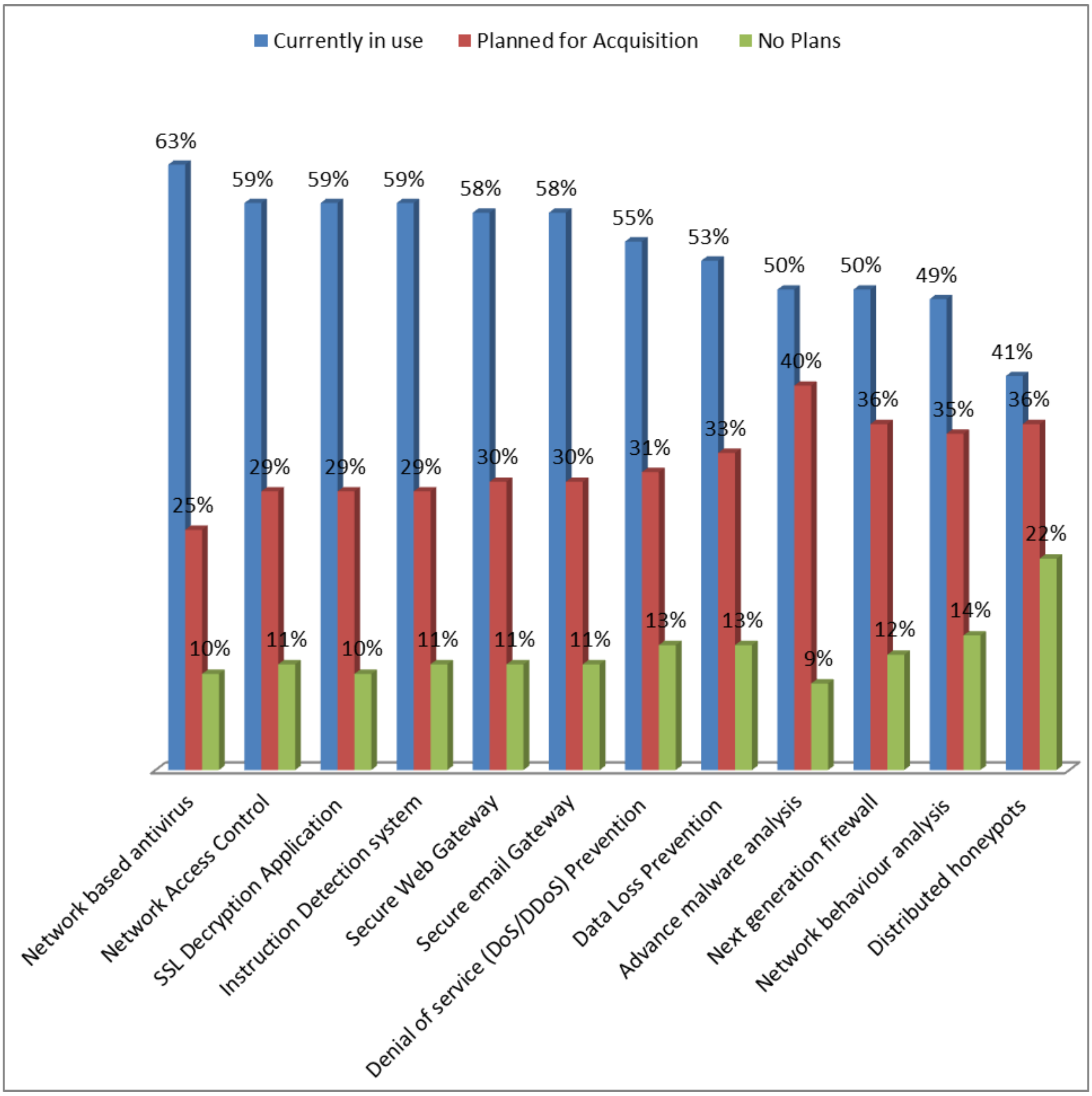
V. PERFORMANCE ANALYSIS OF DIFFERENT NETWORK SECURITY TECHNOLOGIES

The suggested methodology in this paper provides an updated version of the taxonomies provided in [12][15] to categorise Network Protection technology, Web apps and harmful programs, Weaknesses with the highest

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

increased danger, Targets for computer security expenditure this year, and analyze attacks based on types of threats, targeted field, purpose, effect, and incident classifications. Every step of the attack will be broken down into terms that can be grasped.

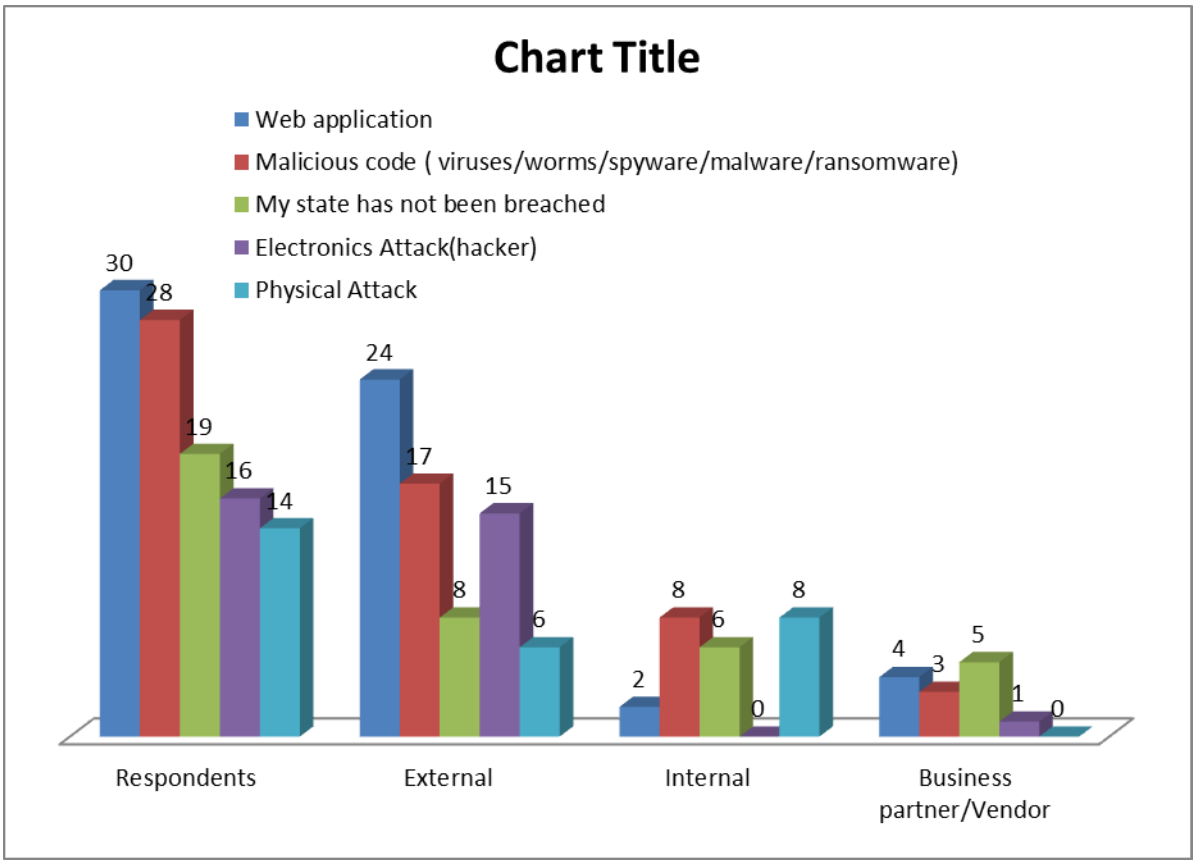
Table 1: Network Security technologies in use and planned for acquisition.



Organizations all over the world are increasing their spending to meet these and other improvements. Nonetheless, projections of data security spending indicate that there are many gaps between economies and sector sizes.

Table:2 Web applications and malicious code are the leading sources of security breaches.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731



Source: -2018 Deloitte-NASCIO Cyber security Study

Table:3 Vulnerabilities with the most increased risk exposure over the past 12 months.

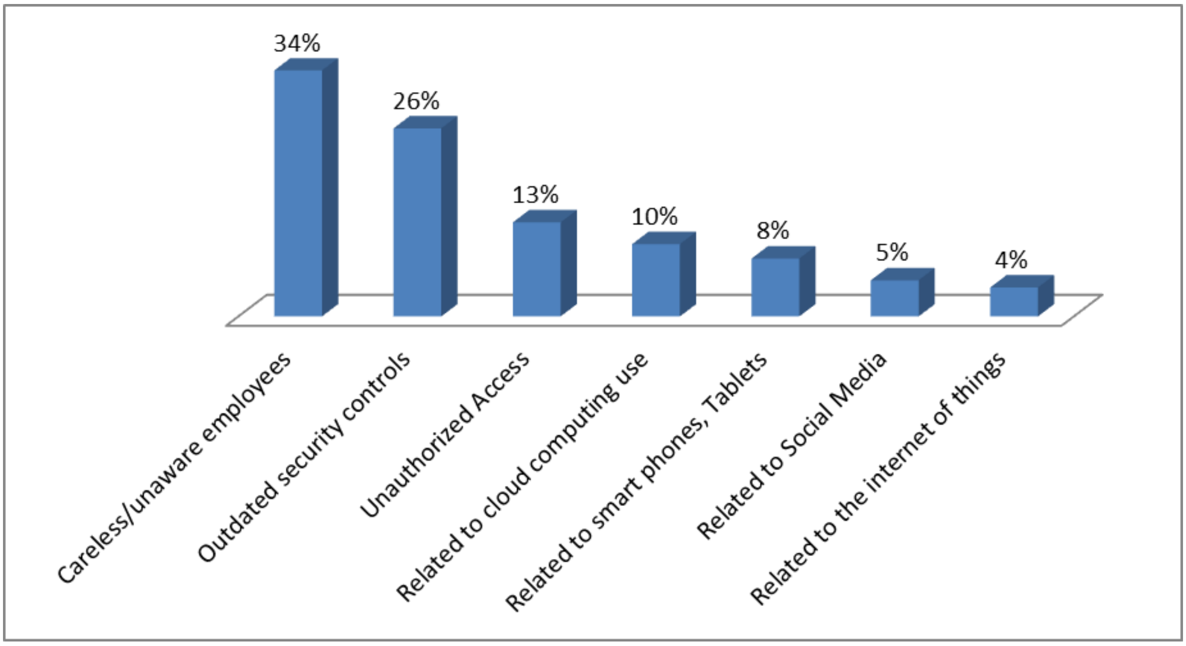


Table:4 Global Information Security Survey 2018-2019

Valuable information to cyber criminals	Targeted attack	Cyber Threats to Organizations	Cyber Threats
Customer information	17%	Phishing	20%

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

Financial information	12%	Malware	20%
Strategic plans	12%	Cyber-attacks (to disrupt)	13%
Board member information	11%	Cyber-attacks (to steal money)	12%
Customer passwords	11%	Fraud	10%
R&D Information	9%	Cyber-attacks (to steal IP)	8%
M&A Information	8%	Spam	6%
Intellectual property	6%	Inter Attacks	5%
Non-Patented IP	5%	Natural Disasters	2%
Supplier Information	5%	Espionage	2%

Cyber protection is based on defending against unwanted and/or accidental access to machines, networks, services, and records. As governments, businesses, and individuals compile, process, and archive large volumes of sensitive information and distribute the data through networks, cyber security has become exceedingly relevant lately. In recent years, data abuses have been almost common place. High-profile cases of cyber hacks have raised the market for advanced tech and defence technologies over the past few years. Global companies are becoming more mindful of the imminent threat, which leads to a larger distribution of capital to companies that help reduce those risks [1].

Although some businesses face cyber threats from particular incidents (about 82% of accommodations industry accidents in 2020 were due to point-of-sale), this table shows that in many respects all sectors are vulnerable to cybercrime [3,4]. As such, there has been a growing need for cyber security services with the sophistication of cyber threats.

Table 5: Industries affected by different types of incidents

Incidents by industry	Crime ware	Cyber Espionage	Denial of service	Energy thing else	Stolen assets	Mics errors	Card skimmers	Privilege misuse	Point of sale	Web applications
Accommodation	5.65	1.88	0.27%	3.49%	1.08%	0.54%	1.61%	0.27%	82.26%	2.96%
Education	6.51	2.40	51.71	16.44	3.42	5.48	0.00	4.11	0.00	9.93
Financial	8.18%	3.51%	56.09%	9.85%	2.65%	3.67%	8.18%	1.50%	0.33%	6.01%
Healthcare	20.51	18.38	0.13	8.39	12.78	24.10	0.67	3.20	0.13	11.72
Information	1.87	0.16	19.06	2.66	0.10	1.12	0.00%	0.13	0.07	74.83
Manufacturing	52.89	4.10	13.78	7.26	2.79	0.56	0.19	15.27	0.00	3.17
Professional	45.59	5.15	19.12	7.54	3.13	5.51	0.00	7.54	0.18	6.25
Public	26.27	45.24	3.08	0.30	16.36	7.78	0.00	0.53	0.00	0.43

Retail	**8.20 %**	**3.47**	**26.81**	**3.79**	**2.21**	**3.47**	**25.55**	**0.00**	**3.47**	**23.03**

The L&G Cyber Protection is one-way investors can get exposure to the cyber security industry. The Cyber Security is the underlying. In order to better understand the factors why cyber security is necessary from an economic point of view, it is necessary to fully identify both the cyber security growth factors and the outlook of the market [8,9]. The accompanying analysis will explore the cyber security growth factors and market outlook and then explain the forms during which the above cyber security index is able to catch these optimistic developments in the field of Cyber Security.

Table :6 Priorities for cyber security investment this year and compared to last year.

Computing security	**High Priority**		**Medium Priority**		**Low Priority**	
	Current Year	Previous Year	Current Year	Previous Year	Current Year	Previous Year
Cloud computing	52%	57%	37%	37%	11%	06%
Cyber security analysis	38%	52%	50%	43%	11%	5%
Mobile computing	33%	35%	52%	58%	16%	7%
Internet of things	25%	29%	27%	61%	48%	9%
Robotics process automation	18%	31%	45%	58%	37%	11%
Machine learning	16%	27%	48%	61%	36%	11%
Artificial intelligence	15%	26%	43%	63%	39%	11%
Bio-matrices	15%	15%	44%	72%	41%	13%
Blockchain	14%	15%	37%	69%	48%	15%

VI. CONCUSION AND FUTURE WORK

A couple of easy measures to safeguard web - based safety and confidentiality. Switch the antivirus on. There seems to be a fair possibility that antivirus software is Pre-installed into machine. If it's not, even if don't find it's enough, there are more than enough free and premium antimalware services to take advantage of. There are usually two ways for advanced antimalware systems to detect and delete ransomware from machine. The first is a basic device search, in which any file on computer is scanned by the antivirus to search for, encrypt, and uninstall malicious software. The second is real-time monitoring, in which running processes and installed files are scanned and identified correctly when they appear on device.A VPN, stands for virtual private network, encrypts all web traffic and routes it to a place of choice via a remote server. Commercial VPNs are generally paying membership utilities which can use it on smartphone by downloading an app. They've got two major results. The first is that, before it hits the VPN registry, all data is safe in an encrypted tube. This stops all of web usage and the final target of r traffic from snooping on ISP and hackers on wi-fi systems. The second is that behind the host address of the VPN, IP address, a unique number which can be used to distinguish device and location, is hidden.This helps to anonymize the actions on the internet. Lots or even hundreds of users are clustered together under a common IP address by most commercial VPNs, making it difficult to track behavior back to a specific user.VPNs could also be used to unfreeze geo-locked content which could only be reached from some nations, like the US Netflix or Hulu web, browser is the window. the world wide web, which can do a variety of activities, but is also susceptible to a wide range of threats and vulnerabilities.

Due to technical developments, cyber threats and cybersecurity have progressed and developed exponentially in the last 20 years. While this is the case, sadly, most organizations have not advanced and are still using cyber defense Such fifth-generation attacks are called huge attacks because they are large-scale and rapidly attacks of the second or third generation, but after the emergence of the fifth generation. This advanced attacker will easily circumvent the traditional, static security mechanisms focused on inspection that are used by most organizations today. Organizations should also adopt a fifth-generation security infrastructure to secure their network networks, cloud and mobile devices in order to defend the most recent threats. In conclusion, there is a need to increase awareness among individuals and organizations about cyber-attacks and their effects, along with security solutions. All can use the app only after evaluating the pros and cons and the violations of protection and precautions must be taken to protect their records. Future research will concentrate on creating a fifth-generation security architecture to secure online platform assets, such as aws, smartphone, and communications infrastructure.

This primer aims to illuminate certain of these similarities. It aims, most of all, to leave two key concepts to the reader. Once and for all, the cyber security dilemma will never be solved. Solutions to the issue, narrow in reach and longevity as they may be, are at least as non-technical in nature since they are technical. It is not only a creative necessity to consider cyber security challenges, but it is also a conservative mission. The exponential advances in technology and facilities are a significant catalyst and driver of cyber security issues, prompting re-evaluation and renewal of structured strategies to address resistant vulnerability interventions. Finally, the emphasis on threat minimization, recovery and removal is the main, core developments and responds to the continuously growing development and development of the defence society's ICT system and architecture. In conclusion, to eliminate competing interests and objectives, these cyber security models need to enhance situational understanding across all circumstances and at all stages.

Reference

[1]. Tarun Dhar Diwan, Dr. Siddhartha Choubey, Dr.H.S.Hota, "Multifactor Authentication Methods: A Framework for Their Selection and Comparison" accepted for publication in International Journal of Future Generation Communication and Networking Vol. 13, No. 3, (2020), pp. 2522–2538, ISSN: 2233-7857 (Web of Science).

[2]. Tarun Dhar Diwan, Dr. Siddhartha Choubey, Dr.H.S.Hota, "A Novel Hybrid Approach for Cyber Security in IoT network Using Deep Learning Techniques" accepted for publication in International Journal of Advanced Science and Technology ISSN:2394-5125, ISSN: 2005-4238 (Scopus indexed Journal).

[3]. Tarun Dhar Diwan, Dr. Siddhartha Choubey, Dr.H.S.Hota, entitled "Development of Real Time Automated Security System for Internet of Things (IoT)" accepted for publication in International Journal of Advanced Science and Technology Vol. 29, No. 6s, (2020), pp. 4180 – 4195, ISSN: 2005-4238 (Scopus indexed Journal).

[4]. Tarun Dhar Diwan, Dr. Siddhartha Choubey, Dr.H.S.Hota, "A Proposed Security Framework for Internet of Things: An Overview" presented in international Conference held on 20-22 December,2019, MTMI, Inc. USA in Collaboration with at amity Institute of Higher Education, Mauritius.

[5]. Tarun Dhar Diwan, Dr. Siddhartha Choubey, Dr.H.S.Hota, "Control of Public Services for Public Safety through Cloud Computing Environment" presented in international Conference held on 04-05 January,2020, Organized by Atal Bihari Vajpayee University, Bilaspur in association with MTMI, USA and sponsored by CGCOST, Raipur (C.G), India.

[6]. Tarun Dhar Diwan, Dr.H.S.Hota, Dr. Siddhartha Choubey "A Study on Security and Data Privacy issues of IoT based Application in Modern Society" presented in international Conference held on 04-05 January,2020, Organized by Atal Bihari Vajpayee University, Bilaspur in association with MTMI, USA and sponsored by CGCOST, Raipur (C.G), India.

[7]. Ten, C. W., Liu, C. C., &Manimaran, G. "Vulnerability assessment of cybersecurity for SCADA systems". IEEE Transactions on Power Systems, 23(4), 1836-1846, 2008.

[8]. J. J. Walker, T. Jones, M. Mortazavi, and R. Blount, "CyberSecurity Concerns for Ubiquitous/Pervasive Computing Environments," 2011 Int. Conf. Cyber-Enabled Distrib. Comput. Knowl. Discov., pp. 274–278, 2011.

[9]. W. B. Miller, D. C. Rowe, and R. Woodside, "A Comprehensive and Open Framework for Classifying Incidents Involving Cyber-Physical Systems," in IAJC/ISAM Joint International Conference, 2014.

[10]. C. Blackwell, "A security ontology for incident analysis," in Proceedings of the Sixth Annual Workshop on CyberSecurity and Information Intelligence Research - CSIIRW "10, p. 1, 2010.

[11]. S. D. Applegate, "The Dawn of Kinetic Cyber," in Cyber Conflict (CyCon), 2013 5th Int. Conference, 2013.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

[12]. P. Bradshaw and P. Bradshaw, Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation, vol. 2017.12. University of Oxford, 2017.

[13]. E. Livanis, “Financial Aspects of Cyber Risks and Taxonomy for the Efficient Handling of These Risks,” in 14thInternational Scientific Conference on Economic and Social Development, 2016, no. May, pp. 80–87.

[14]. M. Khalid, " Cyber Attacks: The Electronic Battlefield", Doha, Qatar Arab Center for Research and Policy Studies2013.

[15]. J. Walker, B. J. Williams, and G. W. Skelton, “Cybersecurity for emergency management,” Technol. Homel. Secur. HST 2010 IEEE Int. Conf., pp. 476–480, 2010.

[16]. Q. Tao, M. Jiang, X. Wang, and B. Deng, “A cloud-based experimental platform for networked industrial control systems,” Int. J. Model. Simulation, Sci. Comput., vol. 9, no. 4, p. 1850024, 2017.

[17]. Al-Mhiqani,M.N., Ahmad R., Abdulkareem K. H., Ali N.S., "Investigation Study of Cyber-Physical Systems: Characteristics, Application Domains, and Security Challenges,"ARPN Journal of Engineering and Applied Sciences, Vol. 12, No. 22, pp. 6557-6567, 2017.

[18]. Y. Biran, J. Dubow, S. Pasricha, G. Collins, and J. M. Borky, “Considerations for Planning a Multi-Platform Energy Utility System,” Energy Power Eng., vol. 9, no. 12, pp. 723–749, 2017.

[19]. W. Wang and Z. Lu, “Cybersecurity in the Smart Grid: Survey and challenges,” Comput. Networks, vol. 57, no. 5, pp. 1344–1371, 2013.

[20]. Ali, N. S., &Shibghatullah, A. S.,"Protection Web Applications using Real-Time Technique to Detect Structured Query Language Injection Attacks," International Journal of Computer Applications, Vol. 149, No. 6, pp. 0975-8887,2016.

[21]. S. K. Venkatachary, J. Prasad, and R. Samikannu, “Economic Impacts of Cyber Security in Energy Sector : A Review,” Int. J. Energy Econ. Policy, vol. 7, no. 5, pp. 250–262, 2017.

[22]. D. E. Denning, “Activism, Hacktivism, And Cyberterrorism: The Internet As A Tool For Influencing Foreign Policy,” in Networks and Netwars: The Future of Terror, Crime, and Militancy, 1999.

[23]. Sridhar, S., Hahn, A., &Govindarasu, M."Cyber–physical system security for the electric power grid". Proceedings of the IEEE, 100(1), 210-224.

[24]. M. Kjaerland, “A taxonomy and comparison of computer security incidents from the commercial and government sectors,” Comput. Secur., vol. 25, no. 7, pp. 522–538, Oct. 2006.

[25]. S. Hansman and R. Hunt, “A taxonomy of network and computer attacks,” Comput. Secur., vol. 24, no. 1, pp. 31–43, Feb. 2005.

[26]. Y. G. B, P. C. Bhaskar, and R. K. Kamat, “Assessing the Guilt Probability in Intentional Data Leakage,” Int. J. Comput. Sci. Inf. Technol., vol. 3, no. 3, pp. 4075, 2012.

[27]. J. Giraldo, E. Sarkar, et al., "Security and privacy in cyber-physical systems: A survey of surveys," IEEE Design & Test, 2017.

[28]. N. S. Ali, “A four-phase methodology for protecting web applications using an effective real-time technique,” Int. J. Internet Technol. Secur. Trans., vol. 6, no. 4, p. 303, 2016.

[29]. K. B. K. B. L. G. Alexander, “Warfighting in Cyberspace,” JFQ NDU Press, vol. 35, no. 46, pp. 58–61, 2007.

[30]. J. R. Klinefelter and T. A. Klinefelter, Minimalist Investor Maximum Profits, 1st editio. Page Publishing Inc, 2015.

[31]. B. Miller and D. Rowe, “A survey SCADA of and critical infrastructure incidents,” in Proceedings of the 1st Annual conference on Research in information technology - RIIT ‟12, 2012, p. 51.

[32]. T. Critchley, High Availability IT Services. Taylor & Francis, 2014.

[33]. A. Rabiah, Y. Zahari, “A Dynamic Cyber Terrorism Framework,” Int. J. Comput. Sci. Inf. Secur., vol. 10, no. Xxx, 2012.

[34]. EIA, “Fuel Oil and Kerosene Sales - Energy Information Administration,” Office of Petroleum and Biofuels Statistics, Office of Energy Statistics, 2013.

[35]. S. Aryan, H. Aryan, and J. A. Halderman, “Internet censorship in Iran : A First look,” 3rd USENIX Work. Free Open Commun. Internet, no. August, p. 8, 2013.

[36]. B. W. O‟Hanlon, M. L. Psiaki, J. A. Bhatti, D. P. Shepard, and T. E. Humphreys, “Real-time GPS spoofing detection via correlation of encrypted signals,” Navigation, vol. 60, no. 4, pp. 267–278, 2013.

[37]. P. Warren and M. Streeter, Cyber Crime & Warfare: All That Matters. Hodder & Stoughton, 2013.

[38]. B. van N. Barend Pretorius, “Cybersecurity and Governance for ICS/SCADA in South Africa" - The Proceedings of the 10th International Conference on Cyberwarfare and Security, in The Proceedings of the 10th International Conference on Cyber, 2015, p. 558.

[39]. W. S. PENDERGRASS, “What is Anonymous?: A case study of an information systems hacker activist collective movement,” 2013.

[40]. D. Wang, Z. Zhang, P. Wang, J. Yan, and X. Huang, “Targeted Online Password Guessing,” Proc. 2016 ACM SIGSAC Conf. Comput. Commun. Secur. - CCS‟16, pp. 1242–1254, 2016.

[41]. W. R. Marczak, J. Scott-Railton, M. Marquis-Boire, and V. Paxson, “When Governments Hack Opponents : A Look at Actors and Technology,” Proc. 23rd USENIX Secur. Symp., pp. 511–525, 2014.

[42]. F. O. H. and M. Sulmeyer, “Getting beyond Norms (New Approaches to International CyberSecurity Challenges),” 2017].

[43]. J E. Grohe, “The Cyber Dimensions of the Syrian Civil War Implications for Future Conflict,” 2015.

[44]. J. Cordy, “The Social Media Revolution: Political and Security Implications,” NATO Parliam. Assem., no. August, p. 10, 2017.

[45]. R. de Oliveira Albuquerque, L. J. GarcÃ-a Villalba, A. L. Sandoval Orozco, R. T. de Sousa JÃonior, and T. H. Kim, “Leveraging information security and computational trust for cybersecurity,” J. Supercomput., vol. 72, no. 10, pp. 3729–3763, 2016.

[46]. C. W. Ten, G. Manimaran, and C. C. Liu, “Cybersecurity for critical infrastructures: Attack and defensemodeling,” IEEE Trans. Syst. Man, Cybern. Part ASystems Humans, vol. 40, no. 4, pp. 853–865, 2010.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731