Journal of Excellence in Computer Science and Engineering, Vol. 3(2) 2017, pp. 1-16

REVIEW ARTICLE

Cyber-Security and Combatting Cyber-Attacks: A Study

[*]C Berin Jones[1]

[1]Professor, Department of Computer Science Engineering, Bhoj Reddy Engineering College for Women, Hyderabad-59, India.

Received- 14 February 2017, Revised- 28 April 2017, Accepted- 14 May 2017, Published- 24 May 2017

ABSTRACT

Cyber-security has turned into a national objective and an administrative need. Expanded cyber-security will help ensure purchasers and organizations, guarantee the accessibility of basic frameworks on which our economy depends, and reinforce national security. In any case, cyber-security endeavours must be precisely custom fitted, keeping in mind the end goal to protect security, freedom, advancement and the open way of the internet which emphasizes on the need for cyber-security. To outline a successful and adjusted cyber-security technique, each piece of the nation's basic framework must be considered independently. Arrangements that might be proper for the control framework or budgetary systems may not be reasonable for securing people in general segments of the internet that constitute the very engineering with the expectation of complimentary discourse basic to our government. Arrangements toward government frameworks can be substantially more prescriptive than arrangement towards private frameworks. The attributes that have made the internet occupy a considerable space- its openness, its decentralized and client controlled nature, and its support for advancement and free expression – might pose considerable hazards if awkward approaches are established that apply consistently to all foundations. This study entails the various perspectives of cyber-security and suggestions for better protection against attacks and techniques which are to be followed by the governmental organizations as counter measures when it comes to cyber-security and cyber-attacks.

Keywords: Cyber-security, Cyber-attacks, Governmental organizations, Counter measures, Preventive techniques.

1. INTRODUCTION

Cyber-security or information technology security are the techniques which are used for protecting computers, networks, programs and data from unauthorized access or attacks that are aimed for exploitation. The counteractive action of harm, unapproved utilization, misuse and the rebuilding of electronic data and correspondence frameworks and the data contained in that to guarantee classification, honesty, and accessibility are all a part of the cyber-security. It incorporates assurance and reclamation of data systems and wire line, remote and satellite systems and control frameworks [1].

Hacking is a straightforward term which implies an unlawful guideline into a PC framework. With an expanding measure of individuals getting associated with web, the security dangers that cause, gigantic damage are likewise increasing [2].

PC security, otherwise called cyber-security or IT security is the assurance of PC frameworks from burglary or harm to the equipment, programming or data, and additionally from disturbance or confusion of the administrations they provide. Cyber-security incorporates controlling physical access to the equipment, and additionally ensuring prevention of mischief that may come through various system modes to get information and perform code infusion. Additionally, due to the inappropriate behaviour by administrators, regardless of whether deliberate or unintentional, IT security is defenceless to being deceived into straying

*Corresponding author. Tel.: +919443123404
Email address: jonesberin@gmail.com (C.B.Jones)
Double blind peer review under responsibility of DJ Publications
https://dx.doi.org/10.18831/djcse.in/2017021001

from secure systems through different strategies. The field is of developing significance because of the expanding dependence on PC frameworks and the internet for the most part of the social orders and remote systems, for example, Bluetooth and Wi-Fi, and the development of "brilliant" gadgets, including cell phones, TVs and minor gadgets as a major aspect of the internet of things.

A cyber-security control contains mandates that defend data innovation and PC frameworks with the reason for compelling organizations and associations to shield their frameworks and data from cyber-attacks. Cyber-attacks include viruses, worms, Trojan horses, phishing, Denial of Service (DoS) attacks, unauthorized access (stealing intellectual property or confidential information) and control framework attacks. There are various measures accessible to avoid cyber-attacks [5]. Cyber-security efforts incorporate firewalls, against infective programming, interruption discovery and anticipation frameworks, encryption and login passwords. There have been endeavours to enhance cyber-security through control and community oriented endeavours among government and the private-segments to urge intentional upgrades to cyber-security. Industry controllers including managing account controllers have considered the hazard from cyber-security and have either started or have a want to start incorporating cyber-security as a part of administrative examinations.

Cyber-security benchmarks (likewise styled cyber-security standards) are strategies for the most part put forward in distributed materials that endeavour to ensure the cyber condition of a client or association. This condition incorporates clients themselves, systems, gadgets, all product forms, data away or travel, applications, administrations, and frameworks that can be associated specifically or by implication to systems. The main goal is to decrease the dangers, including counteractive action or relief of cyber-attacks [6]. These distributed materials comprise of accumulations of tools, measures, security ideas, security shields, rules, chance administration approaches, confirmation and advances.

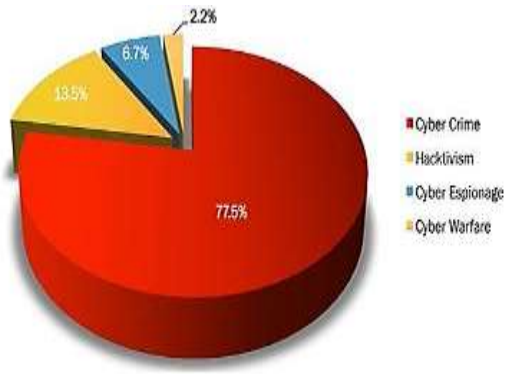
1.1. Rich Rosenthal's cyber assurance program

According to Rich Rosenthal's Cyber Assure Program, the complexity of definition of cyber-security can be drawn as follows.

The mapping as shown in figure B1 draws the complexity of definition. There are seven components, in particular as policy, organization, core, processes, people, skills, and technology, that impact security in the cyberspace. Those components basically have association to each other. They must be produced in one framework to make security in the region of the cyberspace. For instance, individuals as an on-screen character of web utilization, have an aim and aptitude to utilize web in proper ways. In any case, if different components don't bolster their aim, it implies that they can't get any focal points from it or something else. Some of the components of cyber-security issue definition as said in figure B1 are ordered as Extremely Difficult (ED). They are laws, threat/hazard mindfulness, attribution, discouragement, mission confirmation, and flexibility and production network. Different components are named Very Difficult (VD) and Difficult (D). Characterization of those components really demonstrates that cyber-security assumes an imperative part to make "peace" in utilizing web. In fact, it is understood that it is a difficult task to achieve [9].

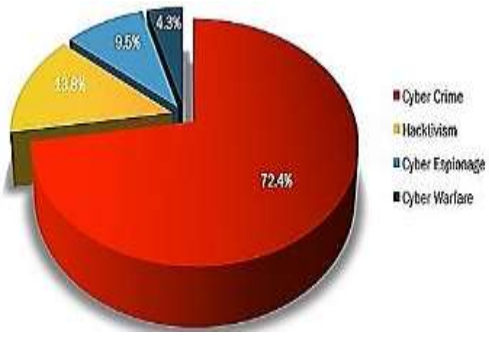
1.2. Motivation behind attacks

The hackers have some motivation behind the cyber-attacks. The below exhibited figures 1(a) to figure 1(e) show the motivation of attacks from 2013 to 2017 descending from 2017.



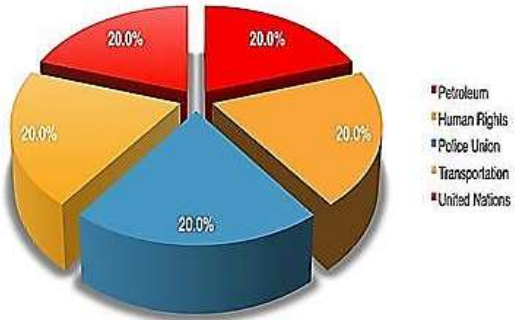
Adapted from [41]

Figure 1(a).Motivation behind attacks in 2017



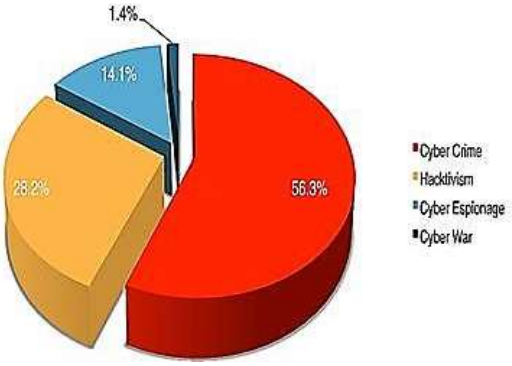
Adapted from [41]

Figure 1(b).Motivation behind attacks in 2016



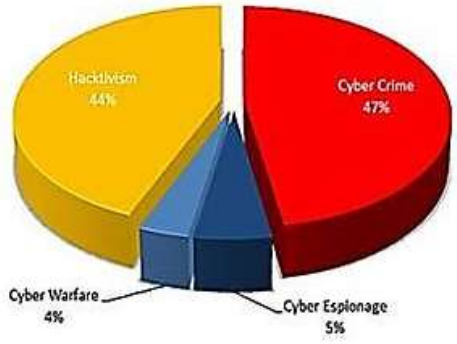
Adapted from [41]

Figure 1(c).Motivation behind attacks in 2015



Adapted from [41]

Figure 1(d).Motivation behind attacks in 2014



Adapted from [41]

Figure 1(e).Motivation behind attacks in 2013

1.3. Cyber-security

It is a term which relates information technology, the internet and virtual reality. Technically it is defined as the assurance of frameworks, systems and information in the cyberspace –a basic issue for all organizations. Cyber-security will just turn out to be more critical as more gadgets are associated with the Internet [8].

While fast innovative advancements have provided vast areas of new opportunity and potential wellsprings of productivity for associations of all sizes, these new advances have additionally brought extraordinary threats.

1.4. Cyber crime

Cyber-crime initially began with programmers attempting to break into PC systems. Some did it only for the excitement of getting to abnormal state security systems; however others looked to increase touchy and grouped activity. In the long run, culprits began to taint PC frameworks with PC infections, which prompted breakdowns on individual and business PCs [10].

PC infections are types of code or malware programs that can duplicate themselves and harm or wreck information and frameworks. At the point when PC infections are utilized on a vast scale, as with bank, government or healing facility organizations, these activities might be arranged as cyber terrorism. PC programmers additionally take part in phishing tricks, such as requesting financial balance numbers, and charge card robbery.

The first recorded cyber-crime took place in the year 1820. The first spam email took place in 1976 when it was sent out over the ARPANT. The first virus was installed on an apple computer in 1982 [12].

1.5. Need for cyber-security

Cyber-security is important since it secures information from strings, for example, information burglary or abuse. Cyber-security includes assurance of delicate individual and business data through counteractive action, identification and reaction to various online attacks. It shields us from basic attacks. Web security handles all the approaching and active information on your PC [13]. Security application in PC needs general updates. An association needs data security for four vital reasons. The requirements for data security are recorded beneath.

- To secure the association's capacity to work.
- To empower the protected operation of users actualized on the association's IT frameworks.
- To secure the information the association gathers and utilizes.
- To protect the innovative resources being used at the association.

2. CYBER-SPACE

The internet is an overall network of PCs and the gear that interfaces them, which by its extreme configuration is free and open to people in general (the Internet). We've turned out to be progressively dependent on the net, and it's being utilized right now to exchange everything from well-disposed messages to touchy information. Every day, there is an expansion in the quantity of dangers against our country's basic frameworks [14]. The associated system of data and interchanges in innovative foundations, including the web, media communication systems, PC frameworks, and inserted processors and controllers in offices and businesses are all possible here.

2.1. Cyber-space and U.S. Bureau of Protection

The U.S. Bureau of Protection noticed that the cyberspace has risen as a national-level worry through a few late occasions of geo-vital noteworthiness. Among those incorporated are, the attack on Estonia's foundation in 2007, purportedly by Russian programmers. In August 2008, Russia again professedly led cyber-attacks, this time in an organized and synchronized dynamic and non-active battle against the nation of Georgia. Expecting that such attacks may lead to a future of fight among countries, the idea of cyberspace operation impacts was expressed [15].

[7] made a nearby estimate of certifiable mission design. This design had experienced survey and had passed the run of the mill security checks, including powerlessness filters. The design had three unmistakable situations: Dev, Test, and Ops (Development, Test, and Flight Operations). A corporate edge firewall encased every one of the three, and there was an extra firewall/bastion as shown in figure B2. The test bed for this experiment was a couple of workstations as of late decommissioned from a flight venture, a few tablets, and a cheap 8-port ethernet centre, facilitating an accumulation of VMs (Virtual machines). One separate physical machine was filled in as a portal between our experiment and the corporate system enabling us to seclude alternate machines and furthermore screen organization's movement. Tests could be kept running with certainty that it would not unintentionally affect the mission machines that were doing the display function.

3. CYBER RISKS AND THREATS

3.1. Cyber risks

Cyber risks can be divided into three distinct types [16]:

- Cyber-crime:

  Directed by people working alone or in sorted out gatherings. Cyber criminals are determined to separate cash, information or bringing on interruption. Cyber-crime can take many structures, including the procurement of credit/charge card information, protected innovation and impeding the operations of a site or administration.
- Cyber war:

  Cyber war is the case in which a country directs damage and secret activities against another country with a specific end goal to bring about interruption or to concentrate information. This could include the utilization of Advanced Persistent Threats (APTs).
- Cyber terror:

  Cyber terror is an association, working freely for a country state, directing fear monger exercises through the medium of the cyberspace.

3.2. Cyber-safety threats

These threats come in the form of computer intrusion (hacking), denial of service attacks, and virus deployment. Because of this problem, various counter measure strategies were framed [16]. These are given under section 6.

- Viruses:

  Viruses contaminate PCs through email connections and record sharing. They erase records, attack different PCs, and make your PC run

gradually. One contaminated PC can bring about problems for all PCs on a system.

- Hackers:

  Hackers are individuals who "trespass" into other PC's from a remote area. They may utilize other PCs to send spam or infections.

- Identity thieves:

  Individuals who get unapproved access to others personal data, for example, social security and money related record numbers. They then utilize this data to perpetrate wrongdoings, for example, misrepresentation or robbery.

- Spyware:

  Spyware is a programming that "piggybacks" on projects users download, accumulates data about online propensities, and transmits individual data without user insight. It might likewise bring about an extensive variety of other PC breakdowns.

4. CYBER ATTACK TOOLS

4.1. Types of cyber-attack tools

Cyber criminals operate remotely, in what is called 'automation at a distance', using numerous types of virus [18]. These include:

- Viruses:
  - Aim: To access, take, change as well as degenerate data and records from a focused on PC framework.
  - Technique: A virus is a little bit of code that can reproduce itself and spread starting with one PC then onto the next by appending itself to another PC record.
- Worms:
  - Aim: To misuse the shortcomings in working frameworks to harm organizations and to convey payloads that permit remote control of the contaminated PC.
  - Technique: Worms are self-reproducing and don't require a program to append themselves to. Worms persistently search for vulnerabilities and report back to the worm creator when shortcomings are found.
- Spyware/adware:
  - Aim: To take control of your PC as well as gather individual data without your insight.
  - Technique: Spyware/adware can be introduced on your PC when you open connections, tap on connections or download tainted programming.
- Trojans:
  - Aim: To make an "indirect access" on your PC by which data can be stolen and harm can be imposed.
  - Technique: A Trojan infection is a program that seems to perform one capacity (for instance, virus expulsion). However really performs malicious action when executed.

4.2. Types of cyber-attacks

Here are eight approaches to guarantee your information is secure [19].

4.2.1. Malware

Malware is a widely inclusive term for an assortment of cyber threats including viruses, worms and Trojans [20]. Malware can be essentially characterized as a code with noxious purpose that regularly takes information or crushes information on the PC.

Working: The way in which the malware enters the system are through email attachments, operating system vulnerabilities or through download of anonymous software.

Anticipation: The most ideal approach to anticipate malware is to abstain from tapping on connections or downloading connections from obscure senders. Such facilitation can be done by conveying strong and refreshed firewalls, which keep the exchange of vast information records over the system to identify and eradicate connections that may contain malware.

Similarly it is imperative to ensure your PC's working framework (e.g. Windows, Linux, X, Mac and OS) which utilizes the most avant-garde security refreshes. Programming

software engineers refresh programs much of the time to discourse any openings or feeble focuses.

4.2.2. Phishing

Regularly acting like a demand for information from a trusted outsider, phishing attacks are sent through email and request that clients tap on a connection and enter their own information. Phishing messages have become substantially more advanced as of late, making it troublesome for a few people to recognize a honest ask for data from a false one. Phishing messages regularly fall into an indistinguishable class from spam and yet are more unsafe than only a straightforward advertisement.

Working: Bulk e-mails which constitute links that may direct the user to a fake site are send. On clicking, fake websites open resulting in the stealing of user information.

Counteractive measures: Confirm any solicitations from establishments that arrive by means of email via telephone. In the event that the email itself has a telephone number, don't call that number, yet focus rather on the one you find freely on the web or inside documentation you've gotten from that organization.

Most organizations are inflexible that they won't request individual data by means of email. In the meantime, most organizations unequivocally prescribe that clients not make touchy data accessible [20].

4.2.3. Password attacks

A secret key attack is the one in which an outsider attempts to access your frameworks by splitting a client's watchword [21].

Working: The technique focuses more on programming that assailants use to attempt and split your secret word. However this product is regularly kept running on all alone framework. Programs utilize numerous techniques to get to accounts, to figure out passwords, and in addition looking at different word blends against a lexicon record.

Counteractive measures: Solid passwords are truly the best way to protect against secret key attacks. This includes the basic password creation strategy. It's prescribed not to utilize words found in the lexicon, regardless of to what extent they are; it just makes the secret key assailant's occupation less demanding. Password changes at regular intervals are also much encouraged.

4.2.4. Denial-of-Service (DoS) attacks

A DoS attack concentrates on disturbing the support of a system. Assailants direct large volumes of information or activity over the system, until the system winds up noticeably with over-burden and can never again work [22].

Working: There are a couple of ways assailants can accomplish DoS attacks, yet the most well-known is the circulated Distributed-Denial-of-Service (DDoS) attack which includes the assailant utilizing different PCs to send the activity or information that will over-burden the framework, without the knowledge of the owner of the PC.

Counteractive measures: The most ideal approach is to upgrade your framework with secure features as conceivable with customary programming refreshes, online security programs, observing and checking your information stream to distinguish any uncommon or debilitating spikes in activity before they turn into an issue. DoS attacks can also be disinfected by dislodging a link or attachment that interfaces the site server to the web.

4.2.5. Man In The Middle (MITM)

MITM can be explained with the following example. For instance, on the off chance that you are managing an account on the web, the man in the centre would speak with you by mimicking your bank, and vice-versa. The man in the centre would then get to the greater part of the data exchanged between both sides, which could incorporate delicate information, for example, financial balances and individual data.

Working: Regularly, a MITM obtains entrance through a non-scrambled remote get to point (i.e. one that doesn't utilize WAP, WPA or WPA2). They would then approach the greater part of the data being exchanged between both sides.

Counteractive measures: The most ideal approach to avert them is to just utilize scrambled remote to focus on WPA security. On the off chance, ensure it utilizes a HTTPS association and consider putting resources into a virtual private Network (VPN). HTTPS utilizes declarations that check the personality

of the servers interfacing with utilizing an outsider organization [23].

4.2.6. Drive-By downloads

It processes through a malware and doesn't require any kind of activity by the client to download [24].

Working: Commonly, a little bit of code is downloaded to the client's framework which inturn connects with another PC to get the rest of the program. It regularly misuses vulnerabilities in the client's working framework or in various projects, for example, Java and Adobe.

Counteractive measures: The most ideal path is to make sure that the majority of the working frameworks and programming projects are up to date. For instance, if your PCs needn't bother with Java or the Flash module, consider uninstalling them.

4.2.7. Malvertising

It is an approach to bargain your PC with vindictive code which enters your framework when you tap on an influenced promotion [25].

Working: Cyber aggressors transfer contaminated show promotions to various destinations utilizing an advertisement organize. These advertisements are then appropriated to locales that correlate specific catchphrases and inquiry criteria. On tapping, some sort of malware will be downloaded.

Counteractive measures: The most ideal approach to avert succumbing to malvertising is to utilize judgment skills. Any promotion that guarantees wealth, free PCs could stow away malware. As usual, up-to-date programming and working frameworks are the best initial line of protection.

4.2.8. Rogue software

They refer to malwares that masquerades as authentic and disguise to be essential for your frame work [26].

Working: Program planners make fly up windows and cautions that look real. These alarms encourage the client to download security programming. By clicking "yes" in such situations, the rebel programming is downloaded to the client's PC.

Counteractive measures: The best safeguard in this case is a refreshed firewall. It is likewise a smart thought to introduce a trusted hostile to infection or against spyware programming program that can distinguish dangers like maverick programming.

Likewise with most sorts of wrongdoing, watchfulness is one of the keys to aversion. As cyber lawbreakers turn out to be more complex and more exchanges move on to the web, the quantity of dangers to individuals and organizations will keep on growing.

4.3. Advanced cyber terrorism tools

The above mentioned cyber-attacks so far exhibited under section 4 are actually the tools used by cyber criminals to perform cyber-crimes. The most advanced cyber-terrorism tools are explained in this section.

4.3.1. Cryptology

Terrorists have started to utilize encryption techniques, voice links that contain data that are encrypted by high frequencies, etc. It would be a Herculean undertaking to decode the data that is sent by terrorists, if they utilize a 512 bit symmetric encryption technique [17].

4.3.2. E-mail related crimes

Usually worms and viruses have to attach themselves to a host programme to be injected. Certain emails are used as host by viruses and worms. E-mails are also used for spreading disinformation, threats and defamatory stuff. The most widely spread email attack as of May 12 2017 is the Ransomware attack "WannaCry" [39].

4.3.2.1. Ransomware attack - WannaCry

The Ransomware has distinguished another variation of "WannaCry" that had the capacity to consequently spread crosswise over huge systems by misusing a known bug in a malignant program. Ransomware has been utilized to send enormous digital attacks, infecting PCs in almost 100 nations [39].

Explores with security organization Avast had watched 75,000 contaminations in 99 nations including Russia, Ukraine and Taiwan. As indicated by reports, the hack constrained British healing facilities to dismiss their patients. It additionally struck Spanish organizations, for example, Telefonia, Portugal Telecom, the conveyance organization FedEx and a Swedish nearby expert. Around 40 National Health Service (NHS) systems in UK were hit by the attack.

Ransomware has attacked India as well. News on May 13, 2017 read that Indian Government had shut down more than 250,000 ATMs across India after WanaCrypt0r Ransomware Cyber Attack. This is exhibited in figure 2 [40].

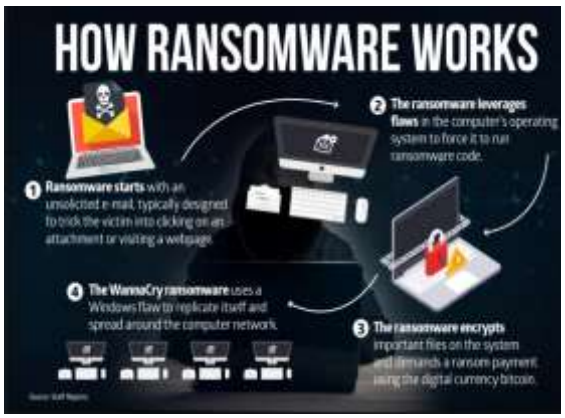
Adapted from [40]

Figure 2.Image of a news report on ransomware attack

Hackers deceived users into opening the noxious malware attachments to spam mails that seemed to contain receipt, job offers, security notices and other authentic documents.

The ransomware rang WannaCry locks records on PCs and scrambles them in a way that it doesn't enable client to get to them any longer. It has been distinguished as an old variation of ransomware that abused a known bug in Microsoft's Windows working framework. At the point when a Windows OS is influenced by the malicious programming, a pop-up window seems to give a detailed clarification on what has happened to your PC, how you can recuperate it and with guidelines on the most proficient method to pay a payoff measure of $300 in Bitcoin. On the left, the pop-up window likewise highlights two countdown clocks, one demonstrating a three-day due date before the sum copies to $600 and another demonstrating a due date when the casualty will lose every one of his information.

The gist on the working of ransomware is exhibited under figure 3.



Adapted from [38]

Figure 3.Working of ransomware

Security specialists say as of now that the attack is sent by means of a worm-a program that spreads without anyone else's input to a system of PCs instead of depending on people to tap on a spam mail or infected attachment. Despite the fact that the malicious program requests a payment measure of cash with a specific end goal to recapture, specialists cautions there is no guarantee that the access would be allowed after making the payment.

Microsoft officially stated that it had included detection and protection against the new malicious programming. Nonetheless, here is a list of measures that can be selected by Windows clients as a safety measure to ensure themselves against the ransomware. The list depends on a few stages given by the Microsoft's Malware Protection Center.

The measures adopted by Microsoft's Malware Protection Center are presented below:

- Introduce and utilize up-to-date antivirus solution, for example, Microsoft Security Essentials or a highly recommendable one.
- Abstain from tapping on suspicious links or attachments or emails from obscure individuals or organizations.
- Install a pop-up blocker on your PCs.
- Have smart screen turned on in Internet Explorer. It will help you recognize reported phishing and malware sites.
- Create regular backup of your important files.

The pictorial scene about the ransomware attack is exhibited in figure 4.

Adapted from [39]

Figure 4.Ransomware attack

6. CYBER SECURITY IN INDIA

6.1. National Information Security Assurance Programme (NISAP)

The fundamental structures and highlights of the projects are:

- Government and fundamental structures should have a security approach and reach [27-32].
- It is required to actualize security control and report any security scene to Indian Computer Emergency Response Team (Cert-In).
- Cert-In needs to make a leading body of evaluator with respect to IT security.
- All associations are to be subjected to an outsider survey from this board consistently.
- Cert-In is to be represented for security consistence on discontinuous premises by the associations.

6.2. Indo-US Cyber Security Forum (IUSCSF)

Under this discussion (set up in 2001) high power assignments from both side met and a few activities were reported [33 – 37]. The highlights are:

- Setting up an India Information Sharing and Analysis Center (ISAC) for better collaboration on anti-hacking measures.
- Setting up India Anti Bot Alliance to bring awareness to light about the developing dangers in the cyberspace by the Confederation of Indian Industry (CII).
- On-going collaboration between India's Standardization testing and Quality Certification (STQC) and the US National Institute of Standards and Technology (NIST) would be extended to new areas.
- The R&D department will deal with the difficult issues of cyber-security, cyber forensics and against anti-spasm research.

7. CYBER ECOSYSTEM

The cyber ecosystem is a worldwide concept and incorporates government and private part data framework; the assortment of connecting people, procedures, data, and correspondence advancements; and the conditions that impact their cyber-security [3]. Basic data framework exists inside the more extensive cyber ecosystem. The country security undertaking will set aside a few minutes in the soundness of the cyber ecosystem, which will be accomplished through enabled people and associations; reliable conventions, items, administrations, setups, and structures; cooperative groups; and straightforward procedures. Besides, the blueprint records four objectives and eleven targets inside the more extensive push to fortify the cyber ecosystem.

7.1. Strengthening cyber ecosystem

Steps to strengthen the cyber ecosystem are,

- Empower individuals and organizations to operate securely.
- Make and use more trustworthy cyber protocols, products, services, configurations and architectures.
- Build collaborative communities.
- Establish transparent processes.

7.2. Conditions for a strong ecosystem

The conditions for a strong ecosystem are,

- Information and correspondence innovation hazard is all around characterized, comprehended and overseen by clients;
- Organizations and people routinely apply security and protection gauges and best practices;
- The personalities of people, associations, systems, administrations, and gadgets are fittingly approved;
- Interoperable security capacities are incorporated with data and correspondence advances; and
- Cyber-physical frameworks.

8. CYBER PHYSICAL SYSTEMS (CPS)

Basic foundations, e.g., the power matrix or water circulation system, are termed the Cyber-Physical Network (CPS).

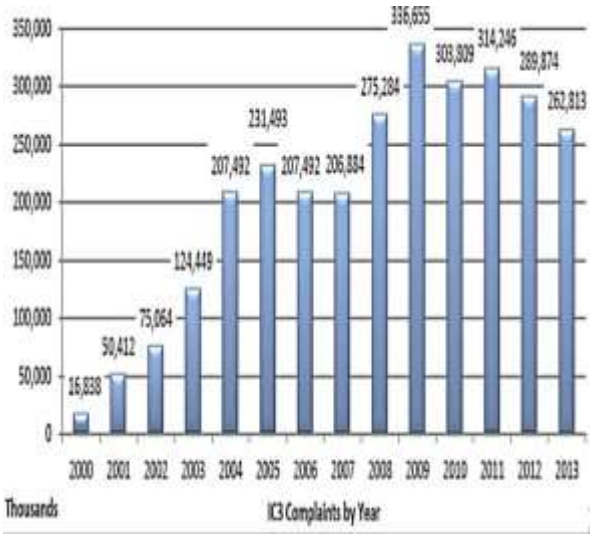
Here physical procedures and segments are associated over data and correspondence innovations (ICT), which are basic for right framework operation. As figuring force and system transmission speeds increment, new applications for modern

control frameworks expand on advances in ICT to enhance the effectiveness of the fundamental physical frameworks. These new applications make a more tight coordination between physical procedures and the cyber-space [4].

It is imperative to dissect the suggestions that expanded utilization of ICT and resultant multifaceted nature has on the wellbeing of these cyber-physical frameworks. This is important to guarantee that security prerequisites are recognized and tended to as a major aspect of the framework configuration handle. The Stuxnet infection or an attack on a German steel process indicated how effective cyber-attacks can bring about physical harm. Moreover, in the vitality space, a multistage cyber-attack could bring about the control of a photovoltaic inverter, changing its dynamic power yield. Cyber-Physical System (CPS) depends progressively on the interconnectivity of gadgets. This brought about expanding consideration for cyber-security nearby customary investigation methods. The introduction of STPA-sec by Young and Leveson (2013, 2014) was an endeavour by the group around STAMP and STPA tending to this necessity. STPA-sec demonstrates that STPA can likewise be utilized to break down the security of frameworks. It switches the conventional base up way to deal with security—where dangers are utilized to determine the security prerequisites — to a top down approach where the results are. A top-down approach could likewise be upheld by other examination procedures [4].

8.1. Unauthorized cyber-physical control

A moderately late conceivable target of the attacker is the unapproved control of cyber physical frameworks. With regards to the associated home prospects of the biological communities, the term cyber physical systems alludes to any computational framework, which shapes some portion of the system additionally and has the capacity to control outer physical infrastructure. This will for the most part additionally have the Remote availability trademark. For instance, cyber physical frameworks incorporate different sorts of (future) keen meters, savvy home apparatuses, for example, brilliant fridges, lighting controllers or warming, ventilation and air-conditioning (HVAC) frameworks, which can control parts of the physical condition. Cyber physical frameworks concentrate on empowering a client to control his or her physical condition and ordinarily give this usefulness through the individual system. Along these lines, unapproved control of digital physical foundation would be a conceivable target for an attack on the individual system. Be that as it may, as the quantity of savvy cyber physical frameworks expands, this attack target is probably going to wind up plainly on a pertinent worry in the associated home biological system prospects. In this way, the short synopsis of some of the dangers introduced above gives a helpful beginning stage for the endeavours to improve the security of present and future individual systems. A portion of the control measures for the recognized dangers are summarized in table A1.



Adapted from [11]

Figure 5.The number of IC3 complaints received from 2000 to 2013

9. REPORTS ON CYBER CRIMES

The Internet Crime Complaint Centre (IC3) built up by NW3C/BJA and FBI-United States of America with the expectation of cyber-crime, discharged its investigation on cyber-crime in 2013. The IC3 was set up on May 8 2000, getting the dissensions of cyber-crime victims over the world. Figure 5 shows the steep increase in the number of complaints, reaching its maximum in 2009 before starting to drop. The IC3 encourages public awareness of how to establish immunity against cyber criminals. In 2013, it received 262,813 complaints with a total dollar loss of $781,841,611, which represents a 48.8%

increase in reported losses over 2012 ($581,441,110) [11].

10. CONCLUSION

Internet has turned into a worldwide wonder; various focal points and hindrances (crimes) are being nurtured and carried out through the web. To adapt to both focal points and detriments, cyber-security is expected to ensure individuals to utilize web securely, specifically the youngsters. Cyber-security covers hardware and programming framework that is supported by national and global methodology and controls. Incorporation of counter measures against cyber-crimes can reduce criminal activity that can affect the country's economy.

REFERENCES

[1] Blueprint for a Secure Cyber Future, The Cyber Security Strategy for the Home Land Security Enterprises, 2011.

[2] G.T.Nojeim, Cybersecurity and Freedom on the Internet, Journal of National Security Law and Policy, Vol. 4, No. 119, pp. 120.

[3] Washington. DC: Cybersecurity Best Practices for Modern Vehicles, National Highway Traffic Safety Administration, 2016.

[4] I.Friedberg, K.McLaughlin , P.Smith , D.Laverty and S.Sezer, STPA-SafeSec: Safety and Security Analysis for Cyber-physical Systems, Journal of Information Security and Applications, 2016, http://dx.doi.org/10.1016/j.jisa.2016.05.008.

[5] B.J.Strawser and D.J.Joy, Cyber Security and User Responsibility: Surprising Normative Differences, 6th International Conference on Applied Human Factors and Ergonomics (AHFE 2015) and the Affiliated Conferences, AHFE 2015.

[6] T.Kawanaka, M.Matsumaru and S.Rokugawa, Software Measure in Cyber-attacks on Production Control System, Computers & Industrial Engineering, Vol. 76, 2014, pp. 378–386, http://dx.doi.org/10.1016/j.cie.2014.08.008.

[7] D.J.Byrne, D.Morgan, K.Tan, B.Johnson and C.Dorros, Cyber Defense of Space-Based Assets: Verifying and Validating Defensive Designs and Implementations, Procedia Computer Science, Vol. 28, 2014, pp. 522 – 530, http://dx.doi.org/10.1016/j.procs.2014.03.064.

[8] E.B.Rice and A.AlMajali, Mitigating the Risk of Cyber Attack on Smart Grid Systems, Procedia Computer Science, Vol. 28, 2014, pp. 575 – 582, http://dx.doi.org/10.1016/j.procs.2014.03.070.

[9] Maskun, A.Manuputty, S.M.Noor and J.Sumardi, Cyber Security: Rule of use Internet SAFELY, Social and Behavioral Sciences, Vol. 103, 2013, pp. 255 – 261, http://dx.doi.org/10.1016/j.sbspro.2013.10.333.

[10] A.Arabo, Cyber Security Challenges within the Connected Home Ecosystem Futures, Computer Science, Vol. 61, 2015, pp. 227 – 232, http://dx.doi.org/10.1016/j.procs.2015.09.201.

[11] A.I.Abubakar, H.Chiroma, S.A.Muaz and L.B.Ila, A Review of the Advances in Cyber Security Benchmark Datasets for Evaluating Data-Driven based Intrusion Detection Systems, Computer Science, Vol. 62, 2015, 221 – 227, http://dx.doi.org/10.1016/j.procs.2015.08.443

[12] V.Alipou, F.Haddadian and H.Maleki, Semantic Reconstruction of Eeconomic Aspect (Cost-Benefit) and Status of Cyber Educations occupation in Iran, Social and Behavioral Sciences, Vol. 46, 2012, pp. 5723 – 5729,

http://dx.doi.org/10.1016/j.sbspro.2012.06.505.

[13] J.Shin, H.Son and G.Heo, Cyber Security Risk Evaluation of a Nuclear I and C Using BN and ET, Nuclear Engineering and Technology, Vol. 49, No. 3, 2017, pp. 517–524, https://doi.org/10.1016/j.net.2016.11.004.

[14] H.Samakas, Counter-measures against Cyber Warfare, Disarmament and National Security Committee, 2015.

[15] D.El-Hmoudova, Motivation and Communication in the Cyber Learning Environment, Social and Behavioral Sciences, Vol. 191, 2015, pp. 1618 – 1622, https://doi.org/10.1016/j.sbspro.2015.04.587.

[16] Z.DeSmit, A.E.Elhabashy, L.J.Wells and J.A.Camelio, Cyber-Physical Vulnerability Assessment in Manufacturing Systems, Procedia Manufacturing, Vol. 5, 2016, PP. 1060–1074, https://doi.org/10.1016/j.promfg.2016.08.075.

[17] V.G.Gopika and Neetha Alex, A Secure Steganographic Method for Efficient Data Sharing in Public Clouds, Journal of Excellence in Computer Science and Engineering, Vol. 1, No. 2, 2015, pp. 11-22, http://dx.doi.org/10.18831/djcse.in/2015021002.

[18] H.Vincent, L.Wells, P.Tarazaga, and J.Camelio, Trojan Detection and Side-Channel Analyses for Cyber-Security in Cyber-Physical Manufacturing Systems, Procedia Manufacturing, Vol.1, 2015, PP. 77–85, https://doi.org/10.1016/j.promfg.2015.09.065.

[19] R.G.Abbott, J.McClain, B.Anderson, K.Nauer, A.Silva and C.Forsythe, Log Analysis of Cyber Security Training Exercises, International Conference on Applied Human Factors and Ergonomics (AHFE 2015) and the Affiliated Conferences, Vol. 3, 2015, pp. 5088 – 5094, https://doi.org/10.1016/j.promfg.2015.07.523.

[20] G.P.Gupta and M.Kulariya, A Framework for Fast and Efficient Cyber Security Network Intrusion Detection using Apache Spark, Procedia Computer Science, Vol. 93, 2016, pp. 824 – 831, https://doi.org/10.1016/j.procs.2016.07.238.

[21] A.S.Bretas, N.G.Bretas, B.Carvalho, E.Baeyens and P.P.Khargonekar, Smart grids cyber-physical security as a malicious data attack: An innovation approach, Electric Power Systems Research, Vol. 149, 2017, pp. 210–219, https://doi.org/10.1016/j.epsr.2017.04.018.

[22] Y.Ashibani and Q.H.Mahmoud, Cyber Physical Systems Security: Analysis, Challenges and Solutions, Computers & Security, Vol. 68, pp. 81-97, https://doi.org/10.1016/j.cose.2017.04.005.

[23] J.Shin, H.Son and G.Heo, Cyber Security Risk Evaluation of a Nuclear I&C Using BN and ET, Nuclear Engineering and Technology, Vol. 49, No. 3, 2017, pp. 517-524, https://doi.org/10.1016/j.net.2016.11.004.

[24] A.Fielder, E.Panaousis, P.Malacaria, C.Hankin and F.Smeraldi, Decision Support approaches for Cyber Security Investment, Decision Support Systems, Vol. 86, 2016, pp. 13-23, https://doi.org/10.1016/j.dss.2016.02.012.

[25] S.Poudel, Z.Ni and N.Malla, Real-Time Cyber Physical System Testbed for Power System Security and Control, International Journal of Electrical Power & Energy Systems, Vol. 90, 2017, pp. 124-133.

[26] T.W.Edgar and D.O.Manz, Science and Cyber Security, Research Methods for Cyber Security, 2017, pp. 33-62, https://doi.org/10.1016/B978-0-12-805349-2.00002-9.

[27] P.H.Nguyen, S.Ali and T.Yue, Model-Based Security Engineering for Cyber-Physical Systems: A Systematic Mapping Study, Information and Software Technology, Vol. 83, 2017, pp. 116-135, https://doi.org/10.1016/j.infsof.2016.11.004.

[28] J.Park, Y.Suh and C.Park, Implementation of Cyber Security for Safety Systems of Nuclear Facilities, Progress in Nuclear Energy, Vol. 88, 2016, pp. 88-94, https://doi.org/10.1016/j.pnucene.2015.12.009.

[29] F.Skopik, G.Settanni and R.Fiedler, A problem shared is a problem halved: A Survey on the Dimensions of Collective Cyber Defense through Security Information Sharing, Computers & Security, Vol. 60, 2016, pp. 154-176, https://doi.org/10.1016/j.cose.2016.04.003.

[30] S.Miller, C.Wagner, U.Aickelin and J.M.Garibaldi, Modelling Cyber-Security Experts' Decision Making Processes using Aggregation Operators, Computers & Security, Vol. 62, 2016, pp. 229-245, https://doi.org/10.1016/j.cose.2016.08.001.

[31] B.Karabacak, S.O.Yildirim and N.Baykal, A Vulnerability-Driven Cyber Security Maturity Model for Measuring National Critical Infrastructure Protection Preparedness, International Journal of Critical Infrastructure Protection, Vol. 15, 2016, pp. 47-59, https://doi.org/10.1016/j.ijcip.2016.10.001.

[32] Y.Vidya and B.Shemimol, Secured Friending in Proximity based Mobile Social Network, Journal of Excellence in Computer Science and Engineering, Vol. 1, No. 2, 2015, pp. 1-10, http://dx.doi.org/10.18831/djcse.in/2015021001.

[33] G.A.Fink, T.W.Edgar, T.R. ice, D.G.MacDonald and C.E.Crawford, Security and Privacy in Cyber-Physical Systems, Cyber-Physical Systems, 2017, pp. 129-141, https://doi.org/10.1016/B978-0-12-803801-7.00009-2.

[34] D.Jin, C.Hannon, Z.Li. P.Cortes, S.Ramaraju, P.Burgess, N.Buch and M.Shahidehpour, Smart Street Lighting System: A Platform for Innovative Smart City Applications and a New Frontier for Cyber-security, The Electricity Journal, Vol. 29, No. 10, 2016, pp. 28-35, https://doi.org/10.1016/j.tej.2016.11.011.

[35] M.Dadkhah, S.A.H.Seno and G.Borchardt, Current and Potential Cyber-Attacks on Medical Journals; Guidelines for Improving Security, European Journal of Internal Medicine, Vol. 38, 2017, 25-29, https://doi.org/10.1016/j.ejim.2016.11.014.

[36] G.L.Kovacich, Establishing a Cyber Security Program and Organization, The Information Systems Security Officer's Guide , Vol. 2016, pp. 131-173, https://doi.org/10.1016/B978-0-12-802190-3.00008-7.

[37] N.Ben-Asher and C.Gonzalez, Effects of Cyber Security Knowledge on Attack Detection, Computers in Human Behavior, Vol. 48, 2015, pp. 51-61, https://doi.org/10.1016/j.chb.2015.01.039.

[38] https://www.google.co.in/imgres?imgurl=http%3A%2F%2Fimg01.ibnlive.in%2Fibnlive%2Fuploads%2F2017%2F

05%2Fransomeware.jpg&imgrefurl=http%3A%2F%2Fwww.news18.com%2Fnews%2Ftech%2Findian-origin-google-techie-links-ransomware-attack-to-north-korea-1402761.html&docid=v59HJ46Xx0GwbM&tbnid=eS1Sq_4POZ_tFM%3A&vet=10ahUKEwjdlIzd1ofUAhUGVbwKHR-mB6g4rAIQMwgUKA4wDg..i&w=1707&h=1040&bih=535&biw=1242&q=ransomware%20attacks%20in%20india&ved=0ahUKEwjdlIzd1ofUAhUGVbwKHR-mB6g4rAIQMwgUKA4wDg&iact=mrc&uact=8.

[39] http://www.deccanchronicle.com/technology/in-other-news/130517/global-ransomware-attack-what-is-it-how-did-it-spread-and-how-to-prevent-it.html.

[40] https://geekboy.co/indian-government-shut-250000-atms-across-india-wanacrypt0r-ransomware-cyber-attack/.

[41] http://www.hackmageddon.com/category/security/cyber-attacks-statistics/.

APPENDIX A

Adapted from [10]

Table A1.Data threats and counter measures

Threat	**Threat Vector**	**Security Measures**
Data exfiltration	Data leaves Home Hub Print screen Screen scrapping Copy to USM keys Loss of backup Email	Data stored in PN and cloud App/device control App/device control Sticky policy for USB transfers Encrypt backups Sticky policy on email control
Data tampering	Modification by another application Undetected tamper attempts Jail-broken device	Application/data sandboxing Logging Dynamic jailbreak detection
Data/device loss	Loss of device Unapproved physical access Application vulnerabilities	Limited data on device and encrypted Device encryption and different Privacy Zones Application sandboxing/patching
Malware	PN OS modification Application modification Virus Rootkit	Managed PN environment Managed applications Dynamic sandboxing- not affect other applications and data

APPENDIX B

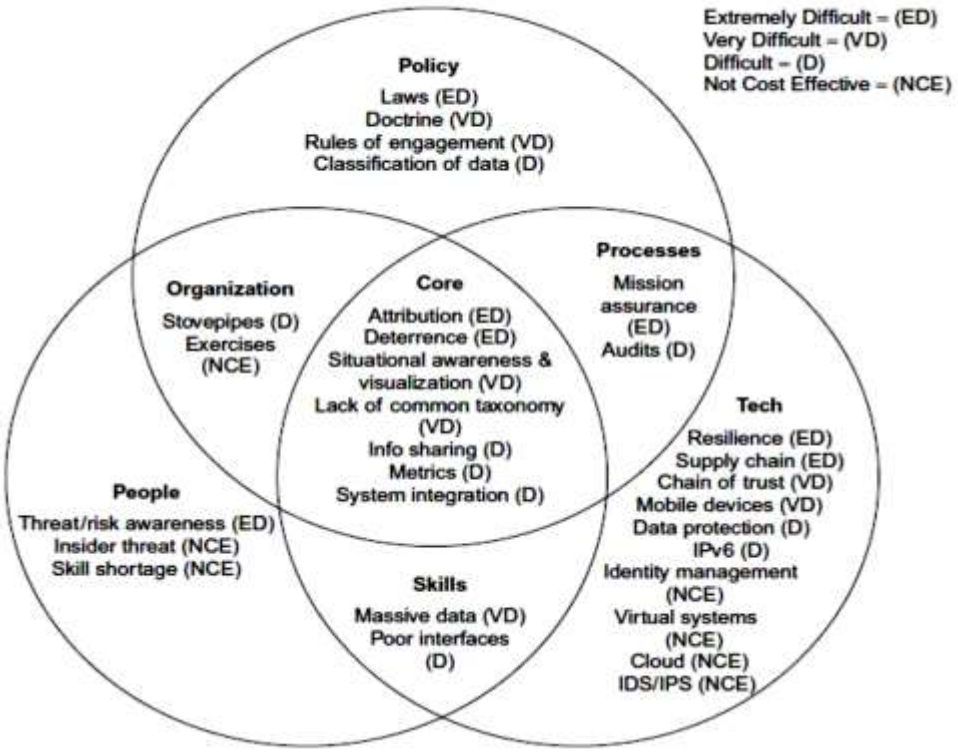
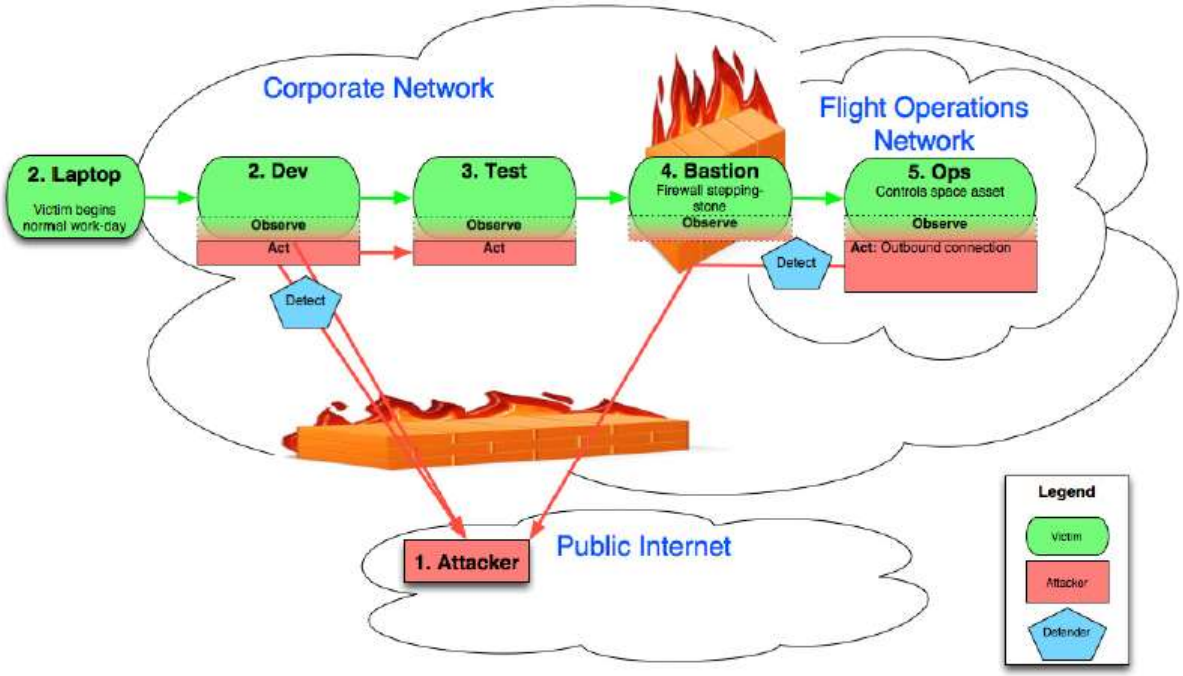


Figure B1.Cyber assurance program



Adapted from [7]

Figure B2.A corporate edge firewall