Analysis on Cyber Security and Its Challenges to Society

Shashank Mishra, Raghav Sandhane
MBA Student, Professor shashank.mishra@associates.scit.edu
Information Technology and Business Management,
Symbiosis Centre for Information Technology, Pune,India

Abstract
Cyber security plays an important role in the field of IT industry and other industry too. Whenever we talk about cyber security, the word cybercrime pops out. Cybercrime is the biggest issues we are facing right now. Every 39 seconds an attacker is hacking something. Since 2008 to 2019 there are more than 8800 data breach cases is being found or filed. Even as we are aware of cybercrime and its stats, only 5% organization are fully secured and other 95% are not fully secured. According to survey 56% organization have weak controls. Basically they are not secured. Apart from taking measures cyber security are facing huge challenges or disturbs to many. This paper mainly focuses on dare to cyber security and also center of attraction is cyber security expertise, morals with changing in technology with time. [1]
Keywords:
Cyber Security, Challenge, Analysis, Morals

1. Introduction

First of all, if we talk about cyber security, we should know what does mean by cyber? Cyber means attribute of culture of computers, information security, data security or virtual reality. Cyber has 284 words related to it. Examples cybernetics, cyberspace, cybercrime etc.

The cyber security term had emerged in 1970s. At that time words such as spyware, phishing, logic bomb, virus did not exist. Since at that time there were no cybercrime. But as years passed this words got in existence due to increase in amount of cybercrime. Now as we know cyber security or in simple words information security plays an important role and is given priority to each organization and various government bodies and agencies.

In 1970s, the computers and internet were under expansion, therefore it was uncomplicated to identify the threat exist in the devices/computers. In 1970s the words like malware and breaches were existed not only to gain financially but also for other purposes. So, there was a German hacker, who hacked the gateway which was situated in the Berkeley so that to connect with 'ARPANET'. German hacker name was "Marcus Hoss". His intention was to hack the Russian computer device and gain the access, make sure that he gets the information about all the spy agents exist in Russia or who works for Russia. He got the access of 400 computer device and basically it was the start of cybercrime. [16]

Cyber security is also known as an information technology security or information security. It is basically to protect the all technology bodies from the attackers or unauthorized access/person. Cyber security also helped in safeguard the networks, programmer, servers or any technical storage from attackers that has stored the crucial information or data. Cyber security plays key role for various government bodies, military which include bodies like CRPF, BSF etc. and large amount of organization. Since they collect the data, process the data and store the data in large amount. Data can be in form of personnel information, financial information, medical information, property related information, assets related information which is critical to organizations to achieve their missions and goals. In today's world or current scenario, a man can transfer their data/information through various modes of channels or mediums just by popping the button/toggle link. Medium can be e-mail or voice message or video. But did he ever think that how securely his data is being transmitted from one place to another place? Did he ever think how data is being sent to other person without leakage of information/Data? Technology and internet is fastest evolving infrastructure in today's time and as on daily basis technology is changing with time furiously. Its changing the mankind or the human race. As technology is changing due to which it becomes difficult to safeguard our private information in constructive or in productive way. In today's time, more than 55% of transaction is online. Surveys shows that the consumption of credit card anticipated to increase from 2018 to 2022, from 20% to 23%. Similarly, for the debit card, it would get increase from 29% to 31%. Consumption of cash is expected to fall down from 33% to 16% during 2018 to 2022. As researcher shows that the world is looking forward to achieve 726 billion transactions using digital payment technology. Hence, cyber security plays key role here. So any technology that contains an information or data needs to be protected from the attackers or any kind of damage or unauthorized access. Each

Manuscript received June 5, 2024
Manuscript revised June 20, 2024
https://doi.org/10.22937/IJCSNS.2024.24.6.17

organization have critical information which they contained in containers. It's called IAP (information asset profiling). In this IAP, organizations have many assets where they contain information. What does IAP do? It helps organizations to find the most critical assets which has most critical information, if it's get hacked by unauthorized person it may cost huge damage to organizations. So organization usually provide highest level of security to those assets which are critical for them. Similarly, government bodies, agencies they have huge amount of data/information's in it, so they require cyber experts to protect their data/information. Since any leakage of information's from government agencies or bodies may cause huge impact or huge loss to particular country. [1]

So, there are diverse in framework that has to followed by different sectors to be secured from attackers.
There is list of some framework-

1. NIST (National Institute of Standards and Technology)
2. NCSP (National Cyber Security Policy)
3. NCSA (National Cyber Security Alliance)
4. FISMA (Federal Information Security Management Act)
5. HIPAA (Health Insurance Portability and Accountability Act)

List goes on and there more than 20000
standards related to cyber security, which helps in securing the organization from any attack.

II. Literature Review

The main aim and motivation to write this research paper is to understand, outline and highlight the current scenario and challenges to the cyber security with increase in modern technology. As a day by day, technology is evolving tremendously and on daily basis new setups and new innovation is coming which has become very complex to handle and also to learn new technology on daily basis is not an easy task. As a new technology is coming, the word risk is also evolving and this risk is major issues to handle by the cyber experts. Here main aim is to understand the challenges faced by cyber experts and why we are still not able to control the cybercrime? Why we are still lacking behind safeguarding our critical assets? How we can overcome this? What are the things needs to remember while protecting an asset from attack? What are the measures needs to be taken when we are aware of threats to an organization? This is what we need to see during the research paper.

In today's era cyber security has become one of the most important field in IT sectors and also in various sectors. Every sectors have a critical data or information on which they run their business and want to achieve their goals and objectives. To run it smoothly and want to make a mark in their business world, you need to have business strategies and make world to believe in your organization, you should have proper security. Because if you are secured, then world is secured. [2]

2.1 What is information security?

Information security is security of critical assets present in the organization, with this information/data they run their business, information security is a security of networks, security of devices like mobile, computers, tabs and each various technology gadgets which are evolving so fast. Information security is a security of data storage devices, security of a cloud and also involve physical security. But from whom? From threats and risks which can be caused by unwanted users and also we can say unauthorized user or from any attacks. How this security issues evolve? This is done by exploiting the vulnerability which can be present in any systems or any applications, through which attackers utilizes the vulnerability or exploits it and process of exploitation of vulnerability is called threat. Vulnerability in a simple word we can say weakness in the systems. When there is a threat, there is a risk. Risk is a product of vulnerability, threats and impact. Security is not a product, it's a process. [3]

2.2 What is technology?

Technology is a branch of knowledge coping with engineering which involves machines, design etc. Now questions arise, how is it impacting cyber security or we can say why there is increase in a cybercrime? Why is it that increase in technology, there is increase in cybercrime or risks towards various technology and IT industry? As we know technology is progressing faster as compare to humans. Some stats show that, the population of world is around 7 billion and facts is more than 3.8 billion people use the internet, which is around 40% of the world population. If you talk about devices which we refer a technology, more than 7.9 billion devices would be connected to internet by 2020. Securing a such amount of devices and data/information is not an easy way from unwanted sources or unauthorized users. This online stature and privacy best opponent is Facebook, WhatsApp, Instagram, Tiktok etc. Since Facebook has 2billion active users, where people usually give their personal data and unknowingly agrees various terms and policy which cause or may cause data breach or may be misuse of personal data which users share on various such Application. This is where awareness about using technology with a security Comes into play. This is where we are lacking behind. There is various technology we are using to protect information or data and detect the Risk developing or threat

evolving around the technology. These technologies are Block chain and Artificial intelligence. Its new era of technology. Now will see how does block chain works and its application? Why everyone is after block chain? [1] [2]

2.3 Blockchain

Blockchain for cybersecurity is a network access control and network segmentation. It can also be micro-segmented network access control. Blockchain was introduced in 2008 and made a huge impact in the various industry. It was developed by **Satoshi** and it was economic revolution. Basically, block chain replaces trust with mathematics. Blockchain was as parallel as a fundamental to internet and has a potential to change our life. Defining as internet behind emails, similarly defining block chain behind bitcoins. Many thinks bitcoin is equal to block chain but it's not. What block chain does? Anyone can transfer money in form of digital without any trust issues and any disintermediation's. Their transactions are blocked in block as in form of cryptography and which is done decentralized computers called as a minors. In block chain, blocks are connected continuously one by one and its becomes difficult for hackers to attacks because if they change one transaction value, then they have to change each transactions of previous blocks which becomes very difficult tasks. Best part is no one owns the chains. Anything that requires database to store the data or ledger can be put on block chain. You don't trust Facebook of world, amazon of world but can trust this technology. Blockchain is an information distribution communication. This technology can solve trust problem and intermediation problem which internet could not solved it. It's a next generation internet with trust and token economics. Blockchain is combination of **Encryption + Distribution** and distributed secured database. How does it work? Strings of blocks, each we recorded data with unified identification (Encrypted). In order to make entry on to block chain database, all computers have to agree about it and its state. So that no computer can make alteration without the consensus of the others. So one of the technology which can be very helpful in cyber security field. Already worldwide spending's on block chain solution is around $2.8 billion. Financial sector is at top of using block chain technology to fight against the cybercrime. Agriculture and food market sector is also using block chain technology and they have spent nearly about $41.9 million. [7] [8]

2.4 What are challenges face by cyber security?

Cyber criminals are using advanced instruments like an Artificial intelligence through which they hack the web and troll the web. As a stats suggest more than 560 websites are developed or introduced per minute. So accidently employees usually post an information on such webs and this thing in coming years will become one of the threat vectors by making use of information or exploiting information via using phishing attacks. Now question arise, who is monitoring continuously and what are the devices that can monitor throughout the period? What are the policies being used by our social media and other media to prevent from attackers?

Secondly, vendor management is an another trend which is being used by many organizations, so that they can focuses on their goals immensely and work towards it. You must be wondering what is vendors? What are their roles? Vendors is any entity that provides materials and services to organizations and outsourcing is identifying a skilled and competent entity that can handle an organizations process. [5]

2.5 Why organizations outsource?

So that can focus on core function, focus on core competence and by vendor outsourcing they actually share a risk. Sources can be of many types from business function outsource to onsite and off-site sourcing. By keeping vendors, organizations only focus on core function and forget about core security policy and its importance. They don't understand the risk and its impact to companies. This is where attackers take advantage and use vulnerability and exploit it. Organizations tends to forget what type of information is shared by them? Tend to forget that how to assess the risk of each vendor? What are the tools that should we use as an organization to prevent from such Risk? Infrastructure and design implementation plays important roles to prevent from threat and risk. If infrastructure and design is strong and well monitored, then chances become less. But usually attackers search vulnerability in infrastructure and design of various bodies and exploit it. Examples you can take Ransomware. Ransomware usually higher as a criminal and they can take over companies, government bodies systems and they hack systems ask for money. Ransomware is one of the biggest threat since 2005 but it has been told first ever ransomware was occurred in 1989 as claimed by Becker's Hospital Review. According to federal government site, in 2014 total thirty-five state reported issue with this attack and also some local bodies reported during that time. At same time some city was exploited by ransomware and the attackers demanded for the $800000. As the years passed, in 2015 it was noticed that there was increase in ransomware attacks and mostly this attacker were targeting the government bodies and education sectors and was demanding the high money. Government sector by 67% and nearly 72% targeted to education sector. There is 600% increase in ransomware attack and its variants. $209 million paid in quarter 1 of 2016 year as a ransom amount to attacker. [2] [5]

As reports suggest since last two years 90% of data is being created and its lots of data and to protect such a huge amount of data we need storage with proper security measures and policies/procedure. But reports tell by 2025 more data will be created in the world and only half of the data will be secured. There are sets of data needs to be security at any cost. Financial transaction, personnel files, medical records and some military intelligence. These are very confidential and sensitive data, if compromised can cause huge impact or loss to society, country and individual. Now question arise, how is data being produced and who is taking care of it? As time is passing, source of data is being changed, also usage and value of data being altered and is shifting from consumer driven data to venture data driven.

Reports said in 2015, data produced by venture is less than 30% but this will change drastically in coming future. Whether data is generated from mobile device, computer, tea shop, coffee shop or from financial services companies, these larger amount of data would become difficult to prevent from an attacker because data is being integrated across various platform/station or channels. Data breaches since 2008 is being increased tremendously and companies are not able store a data securely, because of lack of awareness about cyber security. There is 67% hike in data breaches since 2008 and mostly three sectors have been targeted that is government sector, education sector and medical sector. These breaches can put any company out of their business and also they can have huge impact on their personnel life by reputational loss, financial loss. These can halt the operation of various organization of IT industry. So it's not just technical problem that can be solved by technical person but it requires whole management and each employee working in the organization to cooperate towards the security of an organizations. This is vital to business and also vital to business related customers. So basically big data is big challenge to cyber experts.

As some facts suggests –

- 149,513 email is done in every 60 seconds
- 3.3 million Facebook post is uploaded in every 60 seconds
- every 60 seconds 3.8 million google search is occurred
- 500 hours of YouTube is uploaded in every 60 seconds
- 29 million WhatsApp messages in every 60 seconds
- 448,800 tweets in every 60 seconds, you can imagine amount of data is being created in every 60n seconds. It is said that "1.7megabytes of new information every seconds for every human"
- Another issue related to cyber security is rise in zero-day threats.

2.6 Increase in Zero-Day threats

Firstly, it came into news, in 2010 zero-day vulnerability was occurred and this year also known as "zero-day vulnerability for browser" because most of browser like adobe, flash reader, java, internet explorer was compromised by this attack. Basically zero-day vulnerability attack is an attack that exploits or destroy weakness present in computer software systems. Before developer knows, is being known by attacker and they take advantage of it. To prevent this there is zero-day protection which helps in preventing against the zero-day exploits. Safe computing habit should be followed. To prevent this, we have some tips, that are-

1. Close off public access wherever possible
2. Engage in preventive security practices regularly
3. Ready with your incident response team
4. Defuse and remove unessential software. [15]

So innovation of new technologies is good but to protect them we need to be clear and this is our biggest challenges in this new era of technology. It's possible to secure our systems from cyber-attack or cybercrime from attackers or unwanted users, but we need to aware and make others aware about it. We can be 100% secure. It's just need to learn to be mitigate the risk around our systems. As facts suggest over 750 million malicious attacks occur every year. 2 million per day, 86000 malicious attack per hour, 1500 malicious attack per minute and 24 malicious attack per seconds. There is rise in ransomware attacks, hacktivist, denial of distributed servers attack and most common phishing attack by sending message or personal text to users to steal their sensitive information. So there are basically few challenges like-

1. **Human factors** – Human factors are weakest link in cyber security world, because human leaks their sensitive and their personal information on social media or on various application based software. Experts says "**Professional hacks people**".

For example, password which is most important for anyone to keep it strong so that users can save their personal information and sensitive information from third party or from other user. But we tend to keep password so simple and so predictable that it become very easy for attacker to hack into your system and steal your information. One of cybersecurity blogger said **"Passwords are like underwear's, you don't let people see it, you should change it often, and you should never share it with stranger"** DBIR stats that 81% of data breaches happened due to weak passwords and reused passwords according to DBIR2017. DBIR (2019) suggests the same, 80% data breaches happen due to misuse and weak passwords. Hot targets are your email account and web application account.

Statics credentials are most important key while making strong passwords and also the two-factor authentication. Total number of pawned passwords are 555,278,657, these are real world passwords which were exposed in data breaches.

Top 10 ranked password which are the weakest password –
1. 12345
2. 123456789
3. qwerty
4. password
5. 1234567
6. 12345678
7. 12345
8. iloveyou
9. 111111
10. 123123

so these are the worst password that can be easily predicted and used by attacker to hack into your credential information or systems. [11] [12]

2.7 Internet of Things (IOT)

Iot stands for internet of things and was invented by the **Kevin Asthon,** in 1999 was the first time when world saw the internet was connected with physical world through sensors. An object of Iot can have various features like identity, communication, location, sensors and compute. In Iot, objects are talking to each other and sharing the information amongst them. It is predicted that by 2020 there might be 21 billion Iot devices and you can imagine the whole world will be surrounded by digital devices. What a reach attach surface has been given to attacker? For example, almost all physical devices around you would be talking to each other via internet and sharing information. Car which has the features like- Find my car app, Infotainment, GPS, Internet access, weather, Incident data, safety, Emergency, Road condition and unlock my car app such features can be operated and will become accessible to hacker to attack on system of car and its application. Remote hacking app will be used. Hackers can turn on your wipers through remote access and also can apply breaks. So you can imagine what are the challenges for security experts that they would be facing. Mobile technology is another challenge which is evolving very fast and has various features like Bluetooth, NFC, Wi-Fi through which it makes accessible to hack the mobile device via using hacking tools. As we know even mobile device has a features like accelerometer, Gyroscope, Heart rate, temperature, pressure, Barometer, contacts, proximity, light, location, camera, microphone if mobile is compromised then so many information can be stolen by attacker and this is challenge for cyber experts. [9]

2.8 How to prevent it and what are the measures to be taken by cyber security experts to prevent it from attacker?

Whether it is large business or small business every business needs to have cyber security measures and control to keep their business running by keeping business data safe, by keeping financial transaction safe or we can say its flow, by keeping customers protected online from attacker. What are they-

1. Use well-built passwords- well-built passwords can be made between 8 and 12 characters and always avoid using personal data like date of birth or your pet name etc. Use multi factor authentication and use different password for different accounts to login. Another important point that always change your password in regular interval of time. For example, within 45days or within 90 days etc.

2. Control Access –in organizations admin should take responsibility and authorize each individual can only access data for which they are authorized. You should not allow unwanted people from outside to enter in perimeter area of the organizations. Use segmentation of duties and limit each access to data and service through application based controls.

3. Firewall protection- it is a network security done by monitoring and controlling of incoming and outgoing traffic based on some predefined rules and regulation. It acts like barrier and there are two types that is host based firewall and network base firewall. There are different kind of firewall
a) Proxy firewall which is also called as application based firewall and use 5-layer security protection.
b) Packet filtering firewall which use 4-layer security protection and it checks IP headers, TCP headers. It usually works on network and transport layer. Can block IP address and services.

4. Prefer to use software which are secured and have proper security terms and policy.

5. Always update your software whenever new versions come.

6. Regularly monitor IDS system

7. Spread awareness across the platform wherever possible. Each employee working in the organization should take responsibility to protect their organizations from harmful attacks.

8. We can form cybersecurity policy which are arranged in order of rank. [14]

There are different frameworks which should be implemented by the organizations. Since frameworks are best practices to protect their organizations from threats and risk. Frameworks such as-
1. NIST- stands for national institute of standards and technology which is non-regulatory federal agency with mission of promoting and producing quality of life. How they improve quality of life?
a) They invent
b) They develop
c) They set standards

These framework is form risk management and done by three parts that is-
i) Risk Assessment
ii) Risk mitigation
iii) Evaluation and assessment

There are some questions that every organization should ask to themselves while performing Risk assessment like- what is my risk? What will I do about it? How did I do?
So there are 9 steps for risk assessment in NIST framework.

2. OCTAVE- stands for operationally critical threat, assets and vulnerability evaluation. It is effective security risk evaluation framework which was developed by SEI (software engineering institute) in 2001 at Carnegie Mellon university. There is various version of octave-
a) Octave (1.0) was developed in 1999
b) Octave method (2.0) was developed in 2001, it is basically for large organizations with more than 300 employees.
c) Octave Criteria (2.0) was developed in 2001
d) Octave S (0.9) was developed in 2003, it is for small organizations with less than 300 employees.
e) Octave S (1.0) was developed in 2005
f) Octave Allegro (1.0) was developed in 2007

3. FAIR- stands for factor analysis of information risk. Its main agenda is to make foundation for effective risk management. They are well informed decisions, effective comparison, meaningful measurements, cost-effective risk management and accurate model that can scale in real time and real life. Risk management look after the people, process, policies and technology.

4. ISO 27005.
As an organization if you are outsourcing third party for providing services and materials to you then you should form contract term with third party. For example-

- Level of service and measurement criteria
- Acknowledgment access to IT assets of organizations
- Agree to protect IT Assets of organization
- NDA (non-disclosure agreement)
- Risk assessment and selection of control
- Periodic reporting on control efficiency
- Audit
- Notification of breach and support of independent investigation that no one should interfere while make audit and investigation. Audit bodies and investigation bodies should be independent compare to any bodies.

There are different acts which are there to make organizations to compliance with frameworks and follow it so that they can avoid penalties and protect their business from any harmful activities or any attack. GDPR is a European act and its aims towards preventing & protecting sensitive personal data of people who are residing within EU. Any organizations across the world dealing with personal data of people residing within EU has to follow GDPR act. GDPR has 99 section and each section is well defined regarding the act. Similarly, for India there is act, which is coming that is PDP stands for personal data protection act 2019. It is also called Sri Krishna committee act. It's with the Joint parliament committee and this committee lead by Meenakshi with 10 rajya Sabha members and 20 lok Sabha members. It talks about Indian privacy with 98 section in it. Privacy is very non-organic to India and its people because usually Indian based people share their information with any stranger in one go and which makes them most vulnerable in field of cyber security. So this privacy act will help in many ways. There are five question that each organization should ask to themselves to make cybersecurity as a key dimension in their business continuity management process or procedure-

1. whether cyber-attacks are considered as a top threats to their business continuity plan/process?
2. whether their organization is ready for any cyber-attack?
3. whether the organization evaluate their effectiveness of business continuity process in the circumstances of any cyber-attack?
4. does your organization includes cyber incident as part of disaster process or in case of crisis management plan?
5. Is there any exercise performed between cybersecurity team and business continuity team in case of cyber-attack or in coming cyber-attack and both team perform and validate the scenario together? [6] [13]

III. Cyber ethics

Cyber ethics are nothings but a set of rules and regulations or we can say protocols that should be followed via using internet. If we follow this protocols, then there is good chance that we use internet in proper manner without causing harm to our self and others.

- Always use internet in legal way since internet Is something where you will get large amount of information and use them properly or in legal way.
- Never use others accounts using their credentials.
- Never ever share your information with others on internet because there is high chance that your information can be compromised and might have huge impact.
- Do not make fake accounts and make other one in trouble because of you.
- Please make sure you download those things which are permissible to download.
- Do not send embarrassing picture on internet of others.
- Use information in right way and in right manner.
- Use bandwidth in proper way without wasting them.
- Cyber ethics was invented in 1940 at MIT.
- If you have right to freedom of speech then kindly do not misuse it.

Ethics is all about the rights and wrong. It is a promotion of fairness. What is right or wrong? Ethics also talks about if you know somethings kindly present it, do no hide it. Always stands for right things. Know what ethics of internet are and why they are important at present and in coming future? It is important that cyber ethics should be taught to various schools, colleges and also have seminar in organizations so that people should be aware of it. Awareness is major key role in cybersecurity field. [4] [10]

These are some challenges and solutions by which we can control cyber-crime or we can say minimize the risk. As in cybersecurity field there is no exact solution but we can give our best to prevent and protect our networks, assets, information, data, various technologies, cloud storage, mobile devices, IOT devices etc. from attack or from any kind of threats. Here, need to find gap or reason behind the cyber security challenges faced by cyber experts that why still most of organization is having weak controls and are not able to protect their assets and information.

IV. Research Design

The research design refers to the overall technique that we select to incorporate the various segments of the study in a logic and systematics manner. Ensuring that we can effectively address the examination issue; it sets up the blueprint for the grouping, estimation, analysis and examination of data. The capacity of research configuration is to ensure that the verification got enables us to enough address the analysis issue as unambiguously as could be expected under the circumstances.

The Methodology of this research topic is both Qualitative research just as Quantitative research. Review Research is the furthermost major device for all quantitative research strategies and studies.

As a part of Survey investigation, I have structured the Questionnaire under the direction of my guide Prof. **Raghav Sandhane** and furthermore by experiencing different Research papers and dissecting them. I will send these inquiries to the corporate workers as online Google structures and the outcomes acquired from this encourages me to investigate and arrive at the resolution for my research study.

The Questionnaire incorporates individual inquiries, for example, name, contact subtleties which are discretionary to be filled by the corporates and it additionally contains the inquiries which covers the target of my exploration.

V. Analysis and Findings

Survey questionnaire is floated to the Various IT professional, who are working at top management in information security fields and also to other IT employees who has good amount of experience in IT fields and having good knowledge about information security and its importance.

Questionnaire mainly focuses on following aspects-

- attitude towards information security.
- problems/issues related to security issues.
- do employees receive training related to strength of passwords, complexity and including changing of passwords after certain duration.
- regarding procedure of business continuity plan and recovery plan for virtual systems.
- does organization enforce strong password procedure.
- regarding social engineering awareness and its importance.
- how often does organizations update their antivirus software.
- using same passwords for different accounts.
- which barrier inhibit organization from adequately defending against cyber threats.
- related security budget in organization.
- what is the most critical thing that is holding many organizations back to implementing threat management effectively.
- effectiveness of security training program in organization.

Results were acquired from the IT experts which are organized underneath in a graphical representation.

Current security Training Program in the Organization

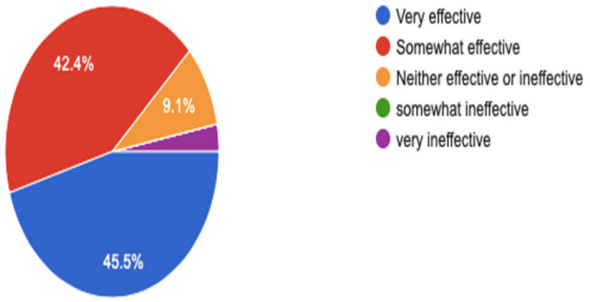

Figure 5.1: current security training program in the organization

As a survey results show, still 42.4% of organization do not have an effective security training program and only 45.5% of organization have effective security program. 3% with very ineffective security training program in their organization.

Most critical barrier holding organization back from implementing threat management more effectively

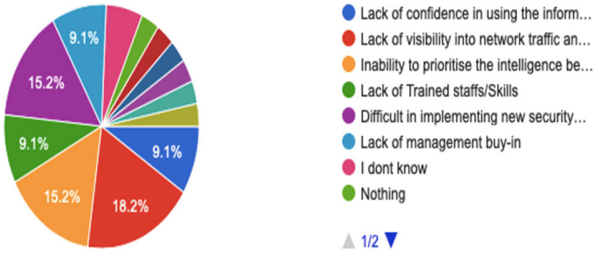

Figure 5.2: Most critical barrier holding organization back from implementing threat management more effectively

Results show, most critical thing which is holding back organizations is a lack of visibility into network traffic and processes with 18.2% and second most critical thing is Difficult in implementing new security systems/tools and Inability to priorities the intelligence being received with 15.2%. Lack of management buy in and lack of trained staffs/skills is at third position with 9.1%.

Attitude towards Information security

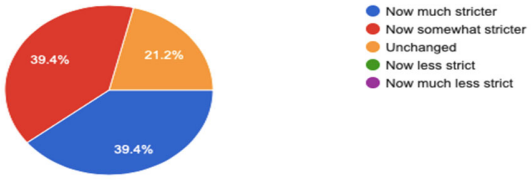

Figure 5.3

Here, 39.4% of organization have strict attitude towards the information security and 39.4% with somewhat stricter. Still 21.2% of organization attitude is unchanged towards information security.

Problems related to Security Measures faced by organizations

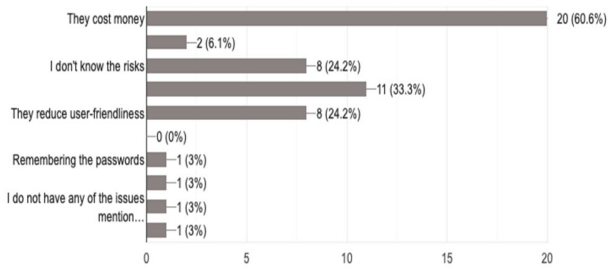

Figure 5.4

Here results show, 60.6% of organization faces issues related to implementing security measures in their organization due to cost. They cost money to them. Second problem, they are time consuming with 33.3%. 24.2% are not aware about the risks.

Do employees receive training related to strength of passwords,
complexity and including changing of passwords after certain duration?

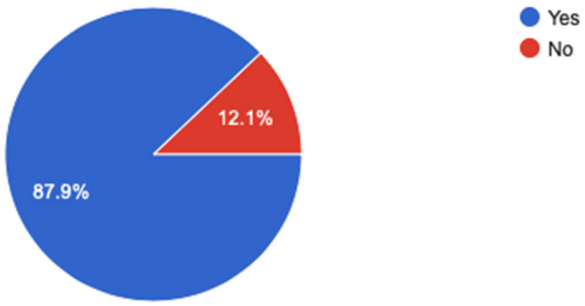

Figure: 5.5

With survey results, we can see here 87.9% of organization conducts training regarding changing of passwords and its importance's. Still 12.1% organization do not conduct training related to it.

Does the Business Continuity Plan spread reinforcement and recuperation methods for every virtual system?

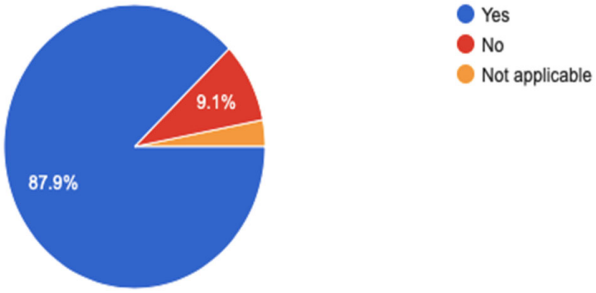

Figure 5.6

We can see from above results that 87.9% of organization do follow procedure or have business continuity plan for recovery and backup in case of some disaster. Still 9.1% don not have business continuity plan.

How are your security assets sourced?

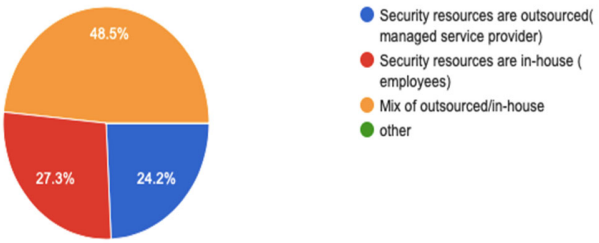

Figure 5.7

Clearly we can see from above results 24.2% of are managed by service providers. Majority of them are mixed of outsourced and in house i.e. about 48.5%.

Is privacy screen is installed on monitor so that they cannot be peered by unauthorized person?

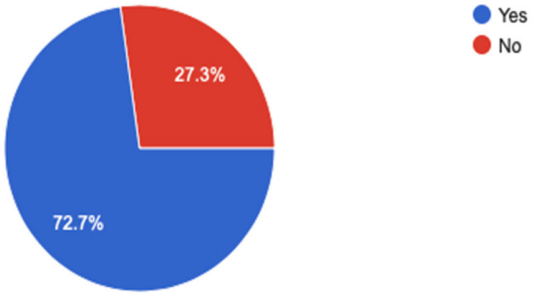

Figure 5.8

What we can see from results shown above is, 72.7% of organization installed privacy screen on their monitor and rest 27.3% of organization, not installed privacy screen on their monitor.

Social engineering awareness and current tactics included in the organization's security awareness training?

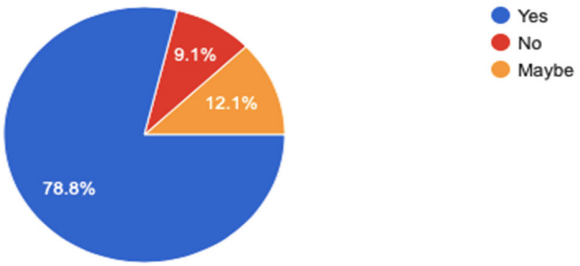

Figure 5.9

From the results, we can conclude that 78.8% organization includes social engineering awareness and current tactics as a part of security awareness training. 9.1% of organization, they do not include it and 12.1% with may be options.

How often do employees update their antivirus software?

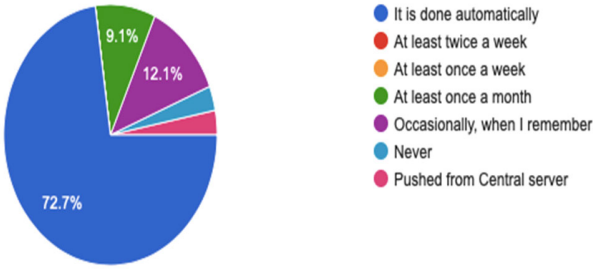

Figure 5.10

We can see from above representation that 72.7% of employees update their antivirus software automatically and whereas 12.1% update their software occasionally when they remember. 9.1% do once a month.

Operating same password for different accounts

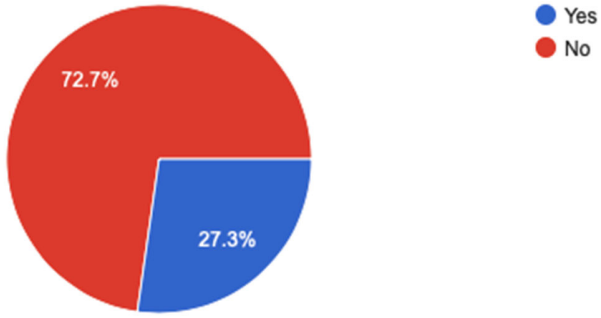

Figure 5.11

With survey results, we can see 72.7% of people operating same passwords and only 27.3% uses different passwords for different accounts.

How's organizations security budget altering in upcoming 12 months?

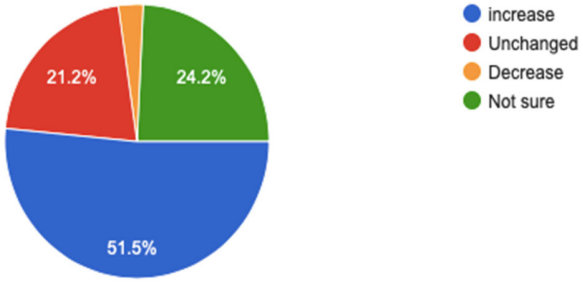

Figure 5.12

From above, we can see 51.5% of organization do have security budget and increasing their budget, understanding the importance of security. Rest, we can see with an unchanged in their budget and 24.2% are not sure about budget related things.

Barriers inhibit your organization from adequately defending against cyber threats?

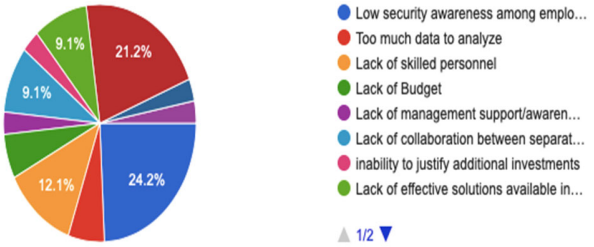

Figure 5.13

Clearly from Results, we can conclude that low security awareness amongst the employee is major reason behind the satisfactorily guarding against cyber threats or cybercrime with 24.2% in the various organization. Excessive amount of data to examine is a second reason with 21.2%. Lack of skilled personnel with 12.1% is third reason and 9.1% due to lack of budget given by organizations. Here are some reasons due to which organization suffers against the cyber threats or cybercrime.

VI. Conclusion

So from above analysis and findings we can conclude that why still organization facing challenges against the cybersecurity. There are some specific reasons why organization facing this issues against cybercrime. They are as follows-

1) lack of awareness amongst the employees working in the organization towards the information security and its importance. Still so

many people who are working in IT companies and other industries not aware about cyber security and its importance. Attitude towards
information security is not changed or somewhat changed. But if you talk about current scenario of world, everything's is going towards digitization. So here importance of cyber security become big and plays important role.
2) Lack of Budgets plays important role while implementing the security controls in the many organizations, especially small and medium size companies.
3) From findings and analyses we found out that majority of people uses same passwords for different accounts, in this case if one of your account is compromised, then all other accounts are in danger or at high risk.
4) Absence or lack of trained staffs is another reason that we are not able to tackle against cybercrime or defend our organization against the cyber threats. Also we found out that, there are more than 200 countries in this world and only 80 countries who has enacted the privacy law and regulation, fighting against this cybercrime. Another prediction is that by 2023, nearly 64% of population will be under some modern privacy law and regulations. So we need to start giving importance and value to cybersecurity and make awareness about cybersecurity and its importance to society as much as possible otherwise will have to face drastic consequences in the coming times.

VII. Future Scope

Cyber security has been acute research area for many years and countless systems and security resolution are accessible on the market these days. But even with these substantial or considerable efforts, cyber attack's, cyber-crime, data breaches happen frequently. This is impacting so many lives physically and mentally include various organization whether they are small or large, impacting them with physical sequel or by financial loss. That unlocked the question why all obtainable defense mechanisms and security structure are fighting against cyber-attacks and why they are at uniform interval of time failing.

VIII. References

[1] International Journal of Scientific & Engineering Research, Volume 3, Issue 6, June-2012 1 ISSN 2229-5518 Study of Latest Emerging Trends on Cyber Security and its challenges to Society by Ravi Sharma.

[2] Cyber Security: Understanding Cyber Crimes- Sunit Belapure Nina Godbole

[3] A Look back on Cyber Security 2012 by Luis corrons – Panda Labs.

[4] (IJSRD - International Journal for Scientific Research & Development| Vol. 4, Issue 04, 2016 | ISSN (online): 2321-0613)-cyber ethics

[5] (International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 7, Issue 4, April 2018, ISSN: 2278 – 1323) ANALYSIS ON CHALLENGES AND THREATS IN CYBER SECURITY)

[6] (Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model) NIST framework

[7] International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-9 Issue-1, October 2019-Alex. R. Mathew (Cyber security through block chain)

[8] Iansiti, Marco, and Karim R. Lakhani. "The truth about block chain." Harvard Business Review 95.1 (2017): pp. 118-127.

[9] Ashton, K. (2009). That 'Internet of Things' thing. RFID Journal,22, 97–114

[10] Cyber ethics 4.0 serving humanity with values by Christoph Stuckelberger / Pavan Duggal (Eds.)

[11] Barton, B.F., Barton, M.S.: User-friendly password methods for computer-mediated information systems. Computer. Secur. 3(3), 186–195 (1984)

[12] Bishop, M., Klein, D.V.: Improving system security via proactive password checking. Computer. Secur. 14(3), 233–249 (1995)

[13] Preprint of the article published in the IET conference proceedings as: Radanliev, P., De Roure, C.D., Nurse, R.C., Nicolescu, R., Huth, M., Cannady, C., Montalvo, R.M., Cannady, S., 2018. Integration of Cyber Security Frameworks, Models and Approaches for Building Design Principles for the Internet-of-things in Industry 4.0, in: Living in the Internet of Things: Cybersecurity of the IoT - 2018. IET, London.

[14] Top steps against cyber(https://www.dell.com/downloads/ca/support/top_10_steps_to_protect_against_cybercrime_dell_en.pdf)

[15] Article Emerging threats by Norton (https://us.norton.com/internetsecurity-emerging-threats-how-do-zero-day-vulnerabilities-work-30sectech.html)

[16] History about cyber security by Sentinel one blog (https://www.sentinelone.com/blog/history-of-cyber-security/)