International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

IJIEMR Transactions, online available on 28th May 2020. Link
:http://www.ijiemr.org/downloads.php?vol=Volume-09&issue=ISSUE-05

Title: CYBER SECURITY IN RECENT TRENDS AND PREVENTIVE MEASURES FROM CYBER THREATS
Volume 09, Issue 05, Pages: 107-115

Paper Authors

MEENA RADHIKA GONGADA, ARAVINDA KUMAR CHALLARAPU, RAVEENDRA REDDY ENUMULA

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

CYBER SECURITY IN RECENT TRENDS AND PREVENTIVE MEASURES FROM CYBER THREATS

[1]MEENA RADHIKA GONGADA, [2]ARAVINDA KUMAR CHALLARAPU, [3]RAVEENDRA REDDY ENUMULA

[1]IBM India Pvt.Ltd, Bangalore, meenasmiles@gmail.com,
[2]IBM india Pvt.Ltd,challarapu@gmail.com,
[3]MPESGI, Guntur Dt, nani.naniravi@gmail.com

Abstract: The main purpose of this paper is to discuss about the importance of the cyber security, how it plays vital role in every one's life in current years and how can we protect ourselves or organization from the cyber-attacks with following minimum precautions in our daily life. The first section of this paper will discuss about the background of the cyber security, in next section cyber security with organizational and individual point of view differently, other sections the ways of cyber-attacks and last section the preventive measures along with action plan for crisis management for cyber threats. Finally, the conclusion of this paper will be expressed in the last section. Cyber security, the terms indicates that safeguarding of all things, which are unprotected or insecurely showing to the Internet, they are our computers, smart devices or phones, individual information, individual's confidentiality and our children's protection. To consider the above things, cybersecurity became growing field, organizations pay more attention and taking precautionary measures to avoid cyber threats. Cyber security is individual responsibility and one should get awareness towards the security measures in terms of connected world now a days as all personal and professional data is at high risk. Organizations (Financial and business sectors) should more focus on security measures also on up to date. They need separate security positions to protect individual and organizational assets, for that one should get trained in the respective areas.

Key Words: Cyber security, Cyber Threat, Crisis Management, Cyber Security techniques, Cyber security by Cloud computing

Introduction: Cyber security is protecting or safeguarding all the connected things via internet, those can be software, hardware, personal data, photos or pictures, smart phones, our financial data.

What is cyber security completely about?

Cybersecurity is an approach for protecting the computers, their connected networks, and the installed programs from cyber threat or digital attacks. These cyberattacks are generally expected at accessing, altering, or abolishing delicate material; most of the times attackers demand money from users if it relates to the individual attacks. If it is organizational attack, they may be chance of impacting the normal business. Cyber

security plays a major role in individual or organizational point of view. In recent years, everyone is living virtually for on-line shopping, connecting to people or posting something on social networking sites and for changing the new job via internet. We do lot of browsing in our day to day life for getting information related to the schools, restaurants, buy or sale property, fund transfer, ticket booking, regular health checkups etc. In all the above cases, we do share lot of personal information most of the times knowingly and sometimes un knowingly. That is the reason sometimes we do get calls from some organizations or promoting company for advertisements, we do wonder "How could someone get my number and keep calling me for advertising?". Then we will be realized we might give or write our information when we visit some restaurant or some other mall for purchase. The discussion so far relates to the individual's security. But if it is same case with Organization, the impact will be huge. We sometimes heard of the cyber-attacks on many organizations and leads to huge loss.

How to accomplish Cybersecurity: In recent years, Security is required for everything whether it is physical or virtually. Cyber Security can be achieved by following minimum tips with maximum vigilance on our daily life.

Below are precautionary measures for achieving the cyber security in individual or an organizational level:

1. **Using the strong passwords:** One should use strong password which are not fall under category of personal information date of birth, surname, Kid's name, Kids date of birth, place of birth. We should adhere to password policy and should change frequently. We should unique passwords which means it should not be used for other accounts. Because if one account attack by the attackers, he/she may attack other accounts easily.
2. **Be more vigilant while using the internet or financial websites outside of the office network:** One should be more alert or vigilant while browsing outside the office network. We should check and understand the features of the browser if any password saving is enabled. We should open the website when it starts with https:// only, mainly for financial websites. The website is safer to open if it starts with https: Always better to "logout "completely from the respective accounts and clear the browsing history. More safety side, we should clear the recycle bin and temp files also.
3. **Importance of antivirus software:** The anti-virus software should be up to date in our computers which will make sure avoid virus attacks or malware attacks. Always consider the auto updates which helps in decrease of the susceptibility to software difficulties. These updates are very much required which was the outcome of latest bug fixes for security weakness provided by respective manufacturer. Most of the security attacks are targeted to the old version of the software computers. Attackers are easily getting the IP address and registry values to attack the computers with the old version software's.
4. **Security concerns related to the social networking:** This is one of most annoying and interesting issue in recent

years as it relates to the social media. Now a day's people are more connected via group chats, different social medial websites for sharing each incident of the life. Ideally speaking most of the teenagers and college going people and few of the other age group people live virtually and get fun and entertainment. But as per the recent surveys, people don't hesitate to share any personal information in social media with the fact of attracting the number people liking post. They share photos of all the occasions of the personal life, different thoughts, activities. Along with that they can have unidentified look into the lives of the others. It is very easy for attackers to get the personal information related to the living place, work place, number of kids, the time of travelling from the current place. Most of the times we hear from the celebrities or Politian's, their accounts are attacked. We hear from our friends their social networking account is hacked by someone who doesn't like them at all. Hence one should understand the significance of the social media, how effectively, securely the usage is being required in all the age groups.

5. One should avoid excessive usage of social media and need to understand importance of posing in social media. Always avoid posting personal information up to date. Due to the popularity of the social media, it is using for immoral purposes most of the times which includes, harassment, sharing of the illegal images of few people or spreading of the rumors. To prevent this, more precautions need to be taking while sharing or posting in social media. In case of, any hacking of the social media account one should contact the proper authorities. Parents should give proper guidance to the teenagers for usage of the social media.
6. **Be more attentive on phishing mails:** We all get phishing mails in one or other time in our daily lives to our personal or official email id. The attackers may target people by sending the phishing mails with the content of sharing of "account information" for receiving the award money, or "download the attachment". Attackers may copy the organizational logo or DSN name for sending the email to get the trust of the receivers. Sometimes these mails may contain the unwanted software which targets for attacking the computers. More attentive or cautious in all the above cases, required to double check the sender email id and take the action accordingly.
7. **Usage of Different Cyber tools and educate towards in their usage:** So far discussed about the different ways of cyber-attacks, all this type of attacks can be overcome by running anti-virus software's, software patches, by installing the different firewalls especially in organization stand point of view will help in protecting the entire networks and connected devices in that network level. There are some security certificates mandatory for some organizations to connect to their network from outside, ideally speaking whichever new system introduced to that network, it should able to acquire the mandatory certificate mentioned by that organization or business unit. These certificates need to be renewed

on yearly or 5 yearly bases based on the certificate definition as per the organizational unit point of view.

How to achieve the Cyber security in Organizational or Business point of view?

Cyber security with respective to the organization or business unit have a lot of significance because any unwanted actions may result into huge business loss or reputation of the business unit. Most of the organizations have their own security policies which adheres to organizational guidelines. Each employee whoever joins they should follow them without any deviation as per the policies.

Different ways of ensuring the Cyber security in organizations:

1. Organizations or Business units themselves have their own network which operates to the respective clients or customers: Companies with number of employees and customers or clients for executing the operational or strategic objectives have common network where others can't log in simply. The network itself has certain firewall to avoid unwanted traffic from outside. The employees should require logging into the common communicator to exchange the any sort of information exchange.

2**. Proper Authentication required to all the people for connecting to the Business network:** One should use proper authentication to log in to the respective network which was allotted by the organization. After going through the proper validations, the employee or concerned team will be allotted the secured credentials. Along with this, Password policy also exists, which means not sharing the password with anyone and password should not fall under any personal data but with a combination of special characters.

3. **Educate the employees in terms of alerting towards the cyber-attacks:** In recent years, organizations pay more attention and more concern for the cyber security within the organization. Frequently monitoring the customer, operational network is being done by respective network security team with in the organization. Employees must go through the security trainings frequently to make sure of more vigilant on cyber threats.

4. **Importance of Data Privacy:** In general, Data privacy or information privacy has used interrelated words. It is one of the features of information technology world, which helps in determining what information can be shared and can't be shared with the outside or third parties in organization by the employees. In data privacy, we have different privacy policies,

- **Privacy related to the browsing information in Internet**: We get various privacy policies while browsing the internet, we do press "agree" or "disagree". These policies are made available for the users to get the permission for using the date for website future usage.
- **Health records privacy:** Usually it works on usage of patient's health records for analysis or publicity purposes. The related health records are subject to strict always that address user access privileges. As per the Law, certain security and validation frameworks are frequently required for

the people that procedure and store the therapeutic records.

- **Financial related data privacy:** It comes to the picture when we do online banking or shopping, all the financial/bank transactions are particularly very much sensible. The respective bank or website must take care all these data privacy policies.

5. **The different levels of access permissions in organizational unit:** The access is provided to the users based on their role in organization for accessing the environment. The roles are mainly "Users", "Administrator", "Special users", based on the role, read or write permissions are provided to the users. This is mainly used for accessing the online documents inside organization and accessing operational(sensible) networks. Because of this access level permissions, someone in the network can't make any mistakes knowingly or un knowingly.

6. **Backing up of the data frequently:** if it is individual or organizational point of view, we should be more alert in backing up of our data or any code. We do have backing up software repositories where the code or documents are safer. Whenever we do make changes in any documents or code in our applications, we must save the changes or check in the changes in the respective repository. If it is our personal computer, the backing up will done by storing into hard disk or uploading into online accounts.in Organizational point of view, Cloud is safer from the security stand point of view.

7. **Maintenance of Secured Wi-Fi networks at workplaces:** Organizations should be more vigilant in providing the work space wi-fi network with more secured way to all the employees.

8. **Restriction of external hard drives usage with official laptops:** By providing the proper access control or restriction towards usage of external drives with official laptops will make sure the data privacy.

Different Cyber security Techniques: By following certain security techniques, we can ensure cyber security. These techniques are used based on the need and the level of security required for that transaction.

1. **Validation Mechanism:** By following strong password mechanism for creating any accounts in online will ensure our account with safer side. If someone tries to hack our account, it is somehow difficult task, if we maintain the strong validation while creating the account. Now a days all the accounts with online access have two-way validation. Most of the times our mobile or smart phone play important role in resetting the password. We should be more careful and keep out smart phone safer side along with the online accounts. Because most of the times, one-time password sends to our mobile number.

Below are the different ways of the two-way validation mechanism:

- **Bio-Metric Identification**: This kind of mechanism is always unique. It states to metric associated to the human characteristics. There are various ways of bio-metric mechanism one can use to identify the individual, "**Fingerprint**", "**FaceRecognition**", "**Retina**", "**DNA**" etc. Using the above bio-metric ways,

one can provide driving license or passport or other country specific identifications.

- **Virtual private network**: In internet, a network is being created safe and secure way by virtual private network. In many bigger organizations have their own VPN mechanism for connecting from the outside. This is always monitored by specific network team closely.

2. **Encryption Mechanism**: It is one way of assuring the confidentialityand authenticity of data. Using different encryption algorithms methods, it is possible for the encryption and decryption as well. Encryption mainly useful for online shopping and online banking. When we purchase something online, we need to provide our card information, personal data over internet. This sensitive information will be transmitted over network using encrypted mechanism. The destination party will require to decrypt the same. As per the researchers," The best and simplest way to protect our self from attacks is MAC of the ciphertext with a secrete or secure message authentication code HMAC-SHA by following certain rules mentioned for that".

a. Encryption done by computing the "Message authentication code" on the ciphertext, but not on the plaintext.
b. Should use two dissimilar keys, one for encryption and other one for the MAC.

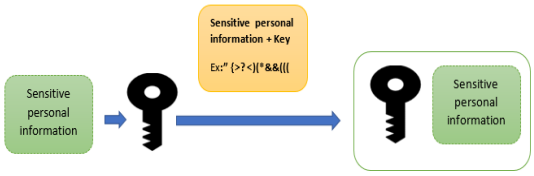

Figure 1, Encryption

3. **Digital Signatures:** It is one of the ways of checking the authenticity of the message. Mathematical scheme is being used for checking the authenticity of the file or digital communications.

Digital signatures classically consist of 3 algorithms:

- Key Generation Algorithm: A digital signature algorithm generates the private key and public key.
- Signing Algorithm: it produces message and a private key which will produces a signature.
- Verification algorithm for Singing: it verifies the public key and signature, it may accept or reject the message as per the authenticity. Example: **RSA algorithm**, **DSA**, **Rabin Signature.**

4. **Antivirus and Firewalls:** It is a type of software intended to forestall, look for, distinguish and evacuate programming viruses and different harmful programming like worms, trojans, adware.

The anti-virus tools are very much important for the users which are required to install, and patches are also needs to be up-to date. Without this antivirus software, our system will affect with the virus with in a minute while we connecting to the

internet. **Firewalls**: It is a system which is designed for preventing an un authorized access from any outside the network. These firewalls are sometimes may be software or hardware or sometimes both. It is networking safety device which monitors the incoming and outgoing data or traffic.

- Proxy servers: These proxy servers act as a gateway for monitoring the incoming or outgoing traffic. In larger organizations, for connecting to the customer or client network, sometimes we must explicitly connect to the proxy server before connecting to the intended applications or servers. It usually has defined credentials for connecting the same.
- Dynamic packet filtering: It is another type of firewall technology where the transmission is happened based on authentic packets for diverse types of networks. It is one of the traditional ways of transmission monitoring mechanism. Example: File Transfer Protocol. This type of protocol works in blocking the traffic depends on the state and the port which is used for transmission and the protocol. This will monitor all the activity from the opening connection till it gets closed.

There are many other firewalls which helps or installed based on the need of the traffic in more secure manner.

Figure 2.Firewall.

Types of cyber-attacks in recent years and lessons learnt from them:

- **Petya (malware):** it is a type of malware. It was spread initially in 2016 through emails, later in 2017 it was spread over as larger global Cyber-attack in various businesses across the global mainly targeted Ukraine and Russia. This cyber-attack was mainly targeted for Windows based operating system which were running with older versions. The effected businesses were running with older version of windows or (Windows XP), failed to update the software patches and updates due to many reasons such as down time for business operations or sometimes it might be compatibility issues. Due to this the entire applications will be vanished since it enters into the NTFS and master file table.
- **WannaCry Cyber Attack:** The affected areas of this attack were Europe, Russia, India and Taiwan. This was also mainly targeted with the organizations of the computers which were running older versions or un supported versions of operating systems with windows XP and windows all the versions.

Sometimes the attack involves in network damage, sometimes the data breach in organizations, viruses can damage computer infrastructure, hacking the passwords for financial data all comes under cyber-attack only. Most of the times the attackers demand the currency in the form of bitcoins to keep the data or applications be safe or free from the cyber-attack. Sometimes companies pay bitcoins to free from their systems or data. But as per the advisors for cybersecurity, experts alerting to the organizations not to pay in the form of bitcoins as it might have lawful consequences.

Impact of the Cyber Attack: After the cyber-attack, business operations will be shut down for few days until the recovery is being done. The attacks are targeting to hit the business continuity for the organizations, it eventually affects the reliability and loss of revenue too. The attack is usually target for damaging the high impacted business applications.

Recovery from the Crisis: Usually backup of the data and changes to the business operation applications happens every day for most of the organizations. Accessing to the impacted servers or impacted computers is not so easy, it requires lot of assistance and guidance from network and infrastructure team. Once we can access to the impacted computers with the help of network and other team, we must follow the below steps.

The primary step in taking the recovery from the crisis management from the business operations side.

- List down the impacted applications based on the priority, High, Medium, Less priority.
- Estimate the amount of time it takes for the recovery from the crisis.
- Estimate the list of the resources required and for the plan of action.
- Must work with business people to synchronize the recovery operations.

Lessons learnt from the Crisis and preventive measures:

- Organizations should be more alert in updating and installing the security updates and patches.
- More efficient in taking the network and data backups on regular basis from all the landscapes, testing and even from the development environments.
- Enhance the test and DR activities: Following proper Disaster recovery planning making sure that data and applications can be restored along with the recovery plan. Sometimes taking the back up on daily basis is more cost effective, we must decide based on our need. If it is fine to take weekly basis, even if we lose the one week's data.

How can cloud computing provides effective solution to the cyber security?

The effective features of cloud computing provide the various advantages towards maintenance for business operations. Since users access the resources in data centers through internet, there is lot of flexibility in accessing them depends on the demand. Cloud security brings numerous levels of controls in infrastructure, database, application, storage. for protection and business continuity. It provides Data security, Regulatory compliance and

protection towards certain types of attacks distributed denial of service attacks.

Conclusion: Cyber security becomes crucial for today's era which ultimately effects the organizations and business operations. Implementing effective cybersecurity procedures is predominantly challenging in now as there are more devices than people, and more over attackers are more innovative. Cyber security is very much sensitive area which involves various technologies which needs to be applied on personal, organizational (private, Government) networks, and on different devices (laptops, Smartphones etc.) as well. Individuals needs to pay more attention towards their own data security. Cyber security is needed for almost all the industries (manufacturer, health care, Financial and govt Sector). Recent days, most of the organizations are appointing chief information security officer to manage their cybersecurity. By following basic security measures will ensure the cyber security most of the times. The organizations should implement their own plan (Business Operations) for protection of data and cyber security. By following list of actions will help in effective crisis identification and recovery planning i.e. Disaster recovery plan should be up to date and systematic testing of backups, with the proper measures, early detection of cyber threat. All these things may or may not prevent the attack, but we may reduce the impact relatively. The research needs to be done on day to day basis by considering the various threat assumptions from outside and efficient recovery methods in case of cyber-attack. It would be helpful for all the business units.

References:

[1] *Goodin, Dan. "Massive espionage malware targeting governments undetected for 5 years". Ars Technica*. Retrieved November 8, 2014.

[2] *"WannaCry Ransomware: What We Know Monday". NPR.org*. Retrieved 2017-05-15.

[3] C. Kaufman, R. Perlman, "Network Security: Private Communication in a Public World", Pearson Education, 2nd edition.

[4] CYBER 2017: The Second International Conference on Cyber-Technologies and Cyber-Systems

[5] "Cloud Computing Security: A Survey ",Issa M. Khalil 1, Abdallah Khreishah and Muhammad Azeem ,

[6] B. Rajkumar, C. Yeo, S. Venugopal, Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility, Future Generation Computer Systems (2009)

[7] National Institute of Standards and Technology, The NIST Definition of Cloud Computing, Information Technology Laboratory.

[8] Cyber Security: Understanding Cyber Crimes- Suneett Belapure Nina Godbole

[9] Computer Security Practices in Non-Profit Organizations – A Net Action Report by Audrie Krause.