Need of Cyber Security And Awareness In Today's Digital Age

Ms. Nimisha D Shetye
Assistant Professor
MKSSS College of Computer Applications For women, Shirgaon, Ratnagiri, India.

Abstract: **Cyber Security plays a vital role in the field of information technology .Cyber security may be referred to as information technology security. Cyber-security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from cyber attacks .Cyber Security is now one of the biggest necessities of the world, because our lives resolve around computers, the cyber-attacks and crimes are dramatically increasing in number every day. Government and various companies are taking many measures in order to prevent these cyber crimes. This paper mainly focuses on challenges faced by cyber security on the latest technologies and need of cyber security and awareness is mentioned.**

I. INTRODUCTION

Technology over the past few decades has become an increasingly integral aspect of today's generation of people. From communicating through instant messages and emails to banking, travelling, studying and shopping, , to professional networking and collaborative work documents, businesses rely on technology to be connected at all times and conduct work effectively , internet has touched every aspect of life. In such technical environment many latest technologies are changing the face of the mankind. But due to these emerging technologies we are unable to safeguard our private information in a very effective way and hence these days' cyber crimes are increasing day by day. Today more than 80 percent of total commercial transactions are done online, so this field required a high quality of security for transparent and best transactions.

Cyber security has become vital for individuals and families, as well as organizations (such as military, government, business houses, educational and financial institutions, corporations and others) that collect and store a wide range of confidential data on computers and transmit that to other computers across different networks. Even the latest technologies like cloud computing, mobile computing, E-commerce, net banking etc also needs high level of security. Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic wellbeing. cyber security is of paramount importance for government organizations also and is a vital asset to the nation. Today many nations and governments are imposing strict laws on cyber securities in order to prevent cybercrimes. Due to growing cyber crimes users should remain vigilant about protecting data. It is essential to understand the varied type of risks and vulnerabilities that exists in the Internet world. For every user, it is important to think before connecting to someone using online medium..Every individual must be made aware about cyber security to save themselves from increasing cybercrime.

II. ISSUES ON CYBER SECURITY TRENDS

Privacy and security of the data will always be top security measures that any organization takes care. We are presently living in a world where all the information is maintained in a digital or a cyber form. Social networking sites provide a space where users feel safe as they interact with friends and family. In the case of home users, cyber-criminals would continue to target social media sites to steal personal data. Not only social networking but also during bank transactions a person must take all the required security measures. Cyber security is the combination of policies and practices to prevent and monitor computers, networks, programs and data from unauthorized access or attacks that are aimed for exploitation. The major areas which are included in cyber securities are as follows:

2.1 Applications

Application security is important because today's applications are often available over various networks and connected to the cloud, increasing vulnerabilities to security threats and breaches. There is increasing pressure and incentive to not only ensure security at the network level but also within applications themselves. One reason for this is because hackers are going after apps with their attacks more today than in the past. Application security testing can reveal weaknesses at the application level, helping to prevent these attacks. Downloadable applications can present many types of security issues for mobile devices. "Malicious apps" may look fine on a download site, but they are specifically designed to commit fraud. Even some legitimate software can be exploited for fraudulent purposes

2.2 Information Security

Strategies for managing the processes, tools and policies necessary to prevent, detect, document and counter threats to digital and non-digital information. Information security programs are built around the core objectives like maintaining the confidentiality, integrity and availability of IT systems and business data. . Sensitive information must be kept - it cannot be changed, altered or transferred without permission. For example, a message could be modified during transmission by someone intercepting it before it reaches the intended recipient.

2.3 Email

Email gateways are the number one threat vector for a security breach. Attackers use personal information and social engineering tactics to build sophisticated phishing campaigns to deceive recipients and send them to sites serving up malware. Email is currently the most common way cyber criminals launch and distribute threats. As the volume of attack has increased so as the level of sophistication. One out of every 412 emails contain a malware attack, 7,710 organizations are hit by a Business Email Compromise attack every month.

2.4 Web Sites and Web server

Websites are always to prone to security risks. Cyber crime impacts your business by hacking your website. Your website is then used for hacking assaults that install malicious software or malware on your visitor's computer. The threat of attacks on web applications to extract data or to distribute malicious code persists. Cyber criminals distribute their malicious code via legitimate web servers they've compromised. But data-stealing attacks, many of which get the attention of media, are also a big threat. Now, we need a greater emphasis on protecting web servers and web applications. Web servers are especially the best platform for these cyber criminals to steal the data. Hence one must always use a safer browser especially during important transactions in order not to fall as a prey for these crimes.

2.5 Social Media Networking

Growing use of soc media will contribute to personal cyber threats. Social media adoption among businesses is skyrocket-ing and so is the threat of attack. In 2012, organizations can expect to see an increase in social media profiles used as a channel for social engineering tactics. To combat the risks, companies will need to look beyond the basics of policy and procedure development to more advanced technologies such as data leakage prevention, enhanced network monitoring and log file analysis.

2.6 Cloud Computing

More firms will use cloud computing. The significant cost savings and efficiencies of cloud computing are compelling companies to migrate to the cloud. Cloud computing presents many unique security issues and challenges. In the cloud, data is stored with a third-party provider and accessed over the internet. This means visibility and control over that data is limited. It also raises the question of how it can be properly secured. It is imperative everyone understands their respective role and the security issues inherent in cloud computing. As cloud use rises in 2012, new breach incidents will highlight the challenges these services pose to forensic analysis and incident response and the matter of cloud security will finally get its due attention.

2.7 Protect systems rather Information

The emphasis will be on protecting information, not just sys-terms. As consumers and businesses are like move to store more and more of their important information online, the requirements for security will go beyond simply managing sys-tems to protecting the data these systems house. Rather than focusing on developing processes for protecting the systems that house information, more granular control will be demanded - by users and by companies - to protect the data stored therein.

2.8 Latest Platforms and Devices

New platforms and new devices will create new opportunities for cybercriminals. Security threats have long been associated with personal computers running Windows. Cyber criminals are increasingly targeting mobile devices and apps. But the prolifera-tion of new platforms and new devices - the iphone, the iPad, Android, for example - will likely create new threats. Mobile devices are small, valuable and we carry them everywhere with us, so their physical security is also an important consideration. Downloadable applications can present many types of security issues for mobile devices. "Malicious apps" may look fine on a download site, but they are specifically designed to commit fraud.

2.9 Everything Physical can be Digital

The written notes on a piece of paper, the report binder and even the pictures on the wall can be copied in digital format and gleaned for the tools to allow a activist-type of security violation, and increasingly this will be a problem.

2.10 Mobile Networks

Today we are able to connect to anyone in any part of the world. But for these mobile networks security is a very big concern. These days' firewalls and other security measures are becoming porous as people are using devices such as tablets, phones, PC's etc all of which again require extra securities apart from those present in the applications used. Mobile networks are highly prone to these cyber crimes a lot of care must be taken in case of their security. Mobile devices typically support cellular networks as well as local wireless networks (Wi-Fi, Bluetooth). Both of these types of networks can host different classes of threats:

Network exploits take advantage of flaws in the mobile operating system or other software that operates on local or cellular networks. Once connected, they can install malware on your phone without your knowledge.

Wi-Fi Sniffing intercepts data as it is traveling through the air between the device and the Wi-Fi access point. Many applications and web pages do not use proper security measures, sending unencrypted data across the network that can be easily read by someone who is grabbing data as it travels.

III. NECESSITY OF CYBER SECURITY

Information is the most valuable asset with respect to an individual, cooperate sector,
State and country with respect to an individual the concerned areas are:

- **For Individuals:** Photos, videos and other personal information shared by an individual on social networking sites can be inappropriately used by others, leading to serious and even life-threatening incidents.
- **For Business Organizations:** Companies have a lot of data and information on their systems. A cyber attack may lead to loss of competitive information (such as patents or original work), loss of employees/customers private data resulting into complete loss of public trust on the integrity of the organization.
- **For Government:** A local, state or central government maintains huge amount of confidential data related to country (geographical, military strategic assets etc.) and citizens. Unauthorized access to the data can lead to serious threats on a country.

IV. EMERGING TECHNOLOGIES FOR CYBER SECURITY

Ours is the age of digital connectivity; we are now on to automating all processes in the business world. Thus the security industry now focuses on building cyber security into applications and the devices that are interconnected. In addition to the basic encryption tools, lots of other security features and tools are now used to ensure comprehensive security. Some emerging technologies that would help secure information systems from hackers in a very effective manner:

Development of user hardware authentication

It is a well-known fact that passwords and usernames used by a majority of data users are weak. This makes it easy for hackers to get access to the information systems and compromise sensitive data of a business entity or government agency. In turn, this has exerted pressure on experts of systems security to come up with authentication methods that are more secure. One of the ways that has been used is the development of user hardware authentication.Tech gurus have developed a solution in the user authentication process with a new Core vPro processor that belongs to the sixth generation of processors. The core vPro can combine different hardware components with enhanced factors simultaneously for user identity validation purposes. Hardware authentication can be especially important when it comes to the Internet of Things (IoT) where the network of connected devices ensures that any device that seeks to be connected has the rights for connectivity to that particular network.

Deep learning

Some technologies are encompassed in deep learning, such as machine learning and artificial intelligence. There is a significant deal of interest for purposes of systems security in these technologies. Deep learning, just like behaviour analytics, focuses on anomalous behaviour. Whenever AI and machine learning systems are fed with the right data regarding potential systems security threats, they can make decisions on how to prevent hacks depending on their immediate environment without any human input. Business organizations and government agencies can now be able to stamp out any persistent or advanced cyber threats using artificial intelligence and machine learning. As you can see, attacks can come from any loose end. It is important to keep up with the latest technologies as to not only stay updated but safe, as well.

V .SECURITY AWARENESS STEPS:

Cyber security awareness promotes foundational understandings on cyber threats and risk, cyber hygiene, and appropriate response options. It informs citizens on best practices and proactive measures when confronted with cyber risks.

The human factor is the weakest link in any information security program. Communicating the importance of information security and promoting safe computing are key in securing a company against cyber crime. Below are a few best practices:

1. Use a ―passphrase‖) and make sure to use a combination of upper and lower case letters, numbers, and symbols to make it less susceptible to brute force attacks. Try not to use simple dictionary words
2. Make sure that you have encryption and password features enabled on your smart phones and other devices.
3. Protecting unauthorized access, disclosure, modification of the resources of the system.
4. Need of separate unit handling security of the organization.
5. Do not click on any links listed in an e-mail message. Copy and paste the URL into your browser.
6. Use and regularly update firewalls, anti-virus, and anti-spyware programs. .
7. Some Elements to Create Awareness in Cyber-Security Educational System In education system, the children must be made aware of the possible attacks and types of intruders. They must also be aware of the terms like: Hardware/Desktop Security, Wi-Fi security, wired security, Password Protection/ (File/Folder) level security, Social networking attacks security and malicious software: • Phishing, Hoaxes • Scare ware, Malware, Virus, Worm, • Trojans, Students are acquiring information technology skills marks question on the educator's abilities to ensure that positive habits of on-line behavior are being formed. Whereas, the teacher giving information about security lacks the knowledge and up-to date information related to Cyber awareness issues, particularly with respect to security. Teacher technology training must be provided for skills development and awareness.
8 Educate your employees and executives on the latest cyber security threats and what they can do to help protect critical information assets The training needs to be updated as new threats emerge and as the business culture and operations change.
9. Use latest emerging technologies in order to protect the information and system.
10 Always adhere to copyrighted information and download games or videos only if they are permissible.

VI. CONCLUSION

Computer security is a vast topic that is becoming more important because the world is becoming highly interconnected, with networks being used to carry out critical transactions. This paper has examined the significance of privacy for individuals as a fundamental human right. Cyber crime continues to diverge down different paths with each New Year that passes and so does the security of the information. This paper also includes the current threats , issues, challenges and measures of IT sector in our society . The latest and disruptive technologies, along with the new cyber tools and threats that come to light each day, are challenging organizations with not only how they secure their infrastructure, but how they require new platforms and intelligence to do so. There is no perfect solution for cyber crimes but we should try our level best to minimize them in order to have a safe and secure future in cyber space. Indian citizens must identify the best techniques in order to protect the information and system, as well as the network in which they work. There is a need of cyber –security curriculum in the near future which will in-build the cyber-security understanding in the current youth and finally the IT sector will get more profound, securely skilled professionals not only in the security sector but also in every sector, thus enhancing the communication, the brain compatibility skills of the employees and the employers.

REFERENCES

[1]IEEE Security and Privacy Magazine – IEEECS "Safety Critical Systems – Next Generation "July/ Aug 2013.
[2] International Journal of Scientific & Engineering Research, Volume 4, Issue 9, September-2013 Page nos.68 – 71 ISSN 2229-5518, "Study of Cloud Computing in HealthCare Industry " by G.Nikhita Reddy, G.J.Ugander Reddy .
[3] Cyber Security: Understanding Cyber Crimes- Sunit Belapure Nina Godbole.
[4] Ravi Sharma, Study of Latest Emerging Trends on Cyber Security and its challenges to Society. International Journal of Scientific &Engineering Research, Volume 3, Issue 6, June-2012, ISSN 2229-5518
[5] Cyber security: challenges for society- literature review.
[6] https://www.tripwire.com/state-of-security/featured/emerging-technology-cyber-security/