ITMR

योगः कर्मसु कौशलम्

WHITE PAPER ON

Cybersecurity

Prepared by **Mohammed Samiuddin**

Contents

Introduction

Cybersecurity is the collection of tools, processes, and practices designed to protect networks, computers, programs, and data from attack, damage or unauthorised access. Today's cybersecurity landscape is an ever-changing environment where the greatest portion of attack is on our day-to-day activities such as email, internet browsing, online transactions, etc. The attackers use mobile apps, e-mail (phishing, spam), the web, and other tools to access intellectual property, personal information, and other sensitive data.

Cyberattacks have increased dramatically over the last decade due to more exposure of personal and business information. This has resulted in disrupting critical operations and imposing high costs on the economy. Cybersecurity refers to the process or mechanism by which the unintended access of information is prohibited. The lack of cybersecurity has been the core reason for increase in Cyberattacks.

Types of Cyberattacks / Threats

There are many methods of cyberattacks such as injecting malware, phishing, stealing data, and so on:

- Cyber Espionage: Refers to the act or practice of obtaining secrets without permission from the information holder
- Internet Crimes: Intentionally harm the reputation of individuals directly or indirectly using modern telecommunication networks such as Internet (chat rooms, emails, notice boards, and groups) and mobile phones (SMS / MMS). It identifies theft, credit card fraud, computer fraud, destruction / damage / vandalism of property, etc.
- Cyber Warfare: Involves actions from a nation-state or international organisation to attack and attempt to damage another nation's computers or information networks through computer viruses or denial-of-service attacks
- Installing Virus or Malware
- Social Engineering: Refers to psychological manipulation of people into performing actions or divulging confidential information (information gathering, fraud, or system access, etc.)
- Compromise data storage

Elements of Cybersecurity

Cybersecurity strives to ensure the attainment and maintenance of security properties of the organisation and user's assets against relevant security risks in the cyber environment. The general security objectives comprise of confidentiality, integrity, and availability. The various elements of cybersecurity are:

- Application Security: Use of software, hardware, and procedural methods to protect applications from external threats
- Information Security: Protecting information and information systems from unauthorised access, use, disclosure, disruption, modification, perusal, inspection, recording, or destruction
- Network Security: Consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorised access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorisation of access to data in a network, which is controlled by the network administrator
- Disaster Recovery / Business Continuity Planning: A Disaster Recovery Plan consists of the precautions taken so that the effects of a disaster will be minimised and the organisation will be able to either maintain or quickly resume the data
- End-User Education: User awareness is a significant part of comprehensive security profile to safeguard an organisation's critical resources and increase overall business performance, because many attack types rely on human intervention to succeed

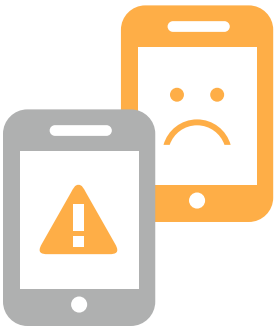
Global Challenges

When computer issues cross international boundaries, the complexity of such issues rise up more and chances of the attackers being brought to the court decreases. This is because different countries have different legal systems and some countries have no laws for computer crime or cybersecurity. It is very easy for attackers to send packets through the Internet from one country to another. But it is very difficult to track attackers because there is no common policy between countries. Most of the attackers are never caught because they change their address and identity, and use different methods to cover their footstep.

The evolution of Internet and technology has resulted in more agile and complex changes and it has become difficult to provide / guarantee complete cybersecurity to a system. Also, lack of specific guidelines for Internet usage has resulted in its misuse.

Solution

The approach to cybersecurity should include a multi-layer architecture, including documented policies and processes. There are laws created for Software Intellectual Property. An intellectual property right refers to a range of intangible rights of ownership in an asset such as a software program. The law provides different methods for protecting the rights of ownership based on their type. Economic Espionage Act 1996 was created by United States Congress to avoid cyber issues. Cybersecurity standards ISO27001 and ISO27031 are important elements in building a strong, resilient information, and communications infrastructure. Government should develop cybersecurity policies in a transparent manner and with relevant stakeholder input. Organisations should be trained to recognise and respond appropriately to social engineering attacks such as, tailgating, phishing, spear phishing, and pharming.



Tips to be secured from Cyberattacks:

At Business

- Conduct risk assessment on cybersecurity
- Derive the IT policies and procedures to be followed
- Ensure the computers and security software's are up to date
- Create awareness to employees and customers on cybersecurity

At Home

- Educate children on: cybersecurity through online games, and social networking safety
- Discuss with the children about their online usage to ensure the sites they visit are safer
- Place the PC or Laptop in a shared space
- Install monitoring tools if the child using computers is below teenage

At Schools

- Ensure the systems and software are updated
- Provide trainings to the students and teachers on cybersecurity

Conclusion

As the number of companies and government organisations throughout the world increased their dependency on computers, the Internet cybercrime has also increased gradually. Cyber criminals target companies or individuals who support other companies to obtain company's data.

There are no borders or discrimination for cybercrime and no single, stand-alone solution for cybercrime due to lack of common policy among different countries. Effective cybersecurity depends on coordinated, integrated preparations for rebuffing, responding to and recovering from a range of possible attacks. The public and the private sector should work closely to implement cybersecurity strategies. Effort should be made to standardise cybersecurity laws across counties. The focus should also be on creating awareness among End-Users.

We can never stop cybercrimes, but with proper strategy, training, and awareness we can secure our networks, computers, programs and data from attack, damage or unauthorised access.

About the Author

Mohammed Samiuddin spearheads the branding aspects & managing client relationships of ITMR. His passion includes speaking on cyber security threats, data security practices and new technological areas.

Reference

http://www.crossdomainsolutions.com/cyber-security/elements

http://securingourecity.org/business

http://securingourecity.org/individuals-family

https://www.paloaltonetworks.com/resources/learning-center/what-is-cyber-security.html

About ITMR

Institute of Technology, Management and Research (ITMR), a division of Mamta Trust, is a premier institute that provides world class professional training programs for the corporates and academic sector. ITMR's motto 'yogah karmasu kausalam' means 'Yoga is excellence in action' and is the foundation of its vision to evolve into a "CENTRE OF EMINENCE" to offer cutting edge vocational skills and mold professionals to become business and technical domain experts. ITMR's professional and corporate training programs include several cutting edge to help working professionals acquire domain expertise and meet the current and emerging challenges in the IT world.

Our flagship training program on Cyber security has (PDCIL) Professional Diploma in Cyber Investigations and Laws is a top of the class cyber security program in the country that trains top officials in the Police departments, Indian and International Banks, Military, Legal fraternity, Fortune 100 Global companies and Blue Chip India IT companies.

ITMR also offers research programs on Cyber Security (network security monitoring and access products), in association with Secure IQ, a leading provider of network security software products with headquarters in Fairfax, Virginia, USA and operations and development in Chennai, India.

Institute of Technology Management & Research
(Division of Mamta Trust)
2/850, Mugaliwakkam Road, Mugaliwakkam, Chennai - 600 125, Tamil Nadu, INDIA.
Admin Office: HTC Towers, No.41, GST Road, Guindy, Chennai – 600 032,
Tamil Nadu, INDIA. Phone: +91 44 4345 3500 / +91 44 4345 3349
Contact for More Information: training@htcitmr.ac.in