International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 05 | May 2019 www.irjet.net p-ISSN: 2395-0072

Cybersecurity: The Agenda for the Decade

Akhandpratap Manoj Singh[1], Shreya Yadav[2], Swaranjali Sharma[3], Suraj Singh Nagvanshi[4]

[1]*Student, Department of Computer Science and Engineering, ABES Engineering College, Ghaziabad, India*
[2]*Student, Department of Information Technology, ABES Engineering College, Ghaziabad, India*
[3]*Student, Department of Electrical and Electronics Engineering, ABES Engineering College, Ghaziabad, India*
[4]*Student, Department of Computer Science and Engineering, ABES Engineering College, Ghaziabad, India*

Abstract - *Cybersecurity: The Agenda for Decade, this paper is aimed particularly at readers concerned with major systems deployed in medium to large commercial or industrial enterprises. It examines the nature and significance of the various potential attacks, and surveys the defence options available. It concludes that Information Technology owners need to think of this threat in more global terms, and to provide a new focus and priority to their defence. Impromptu action will ensure a major improvement in IT resilience at a modest marginal cost, both in terms of finance and in terms of normal IT operation. Cybersecurity plays a key role in the development of information technology services as well as Internet services. Our attention is drawn on "Cybersecurity" when we hear about "Cybercrimes" in day to day life from being in printed media to digital media. Our first thought on "National Cybersecurity" therefore begins on how good is our infrastructure for handling "Cybercrimes".*
India, being a nation which houses 1.3 billion people, more than 1 billion mobile phone connections that's 902 connections per 1000 people, about 730 million Internet Connections by 2020 of which 175 million online shoppers accounting for 70% of ecommerce traffic through Mobile Devices and a rapid increase in Internet uses in Rural part of country makes is important to study and take Cybersecurity seriously [1].

***Key Words*: Security, Cybersecurity, Cyberspace, Cybercrime, Cryptography, Network, Systems, Crime, Protection, e-commerce, Information Technology, Cyber, Mobile, Computer, Internet.**

1.INTRODUCTION

Cybersecurity is the body of technologies, practices and processes designed & developed to protect computers, servers, mobile devices, networks, programs and data from malicious cyberattacks, damage or unauthorized access and help to maintain the integrity of data. Cybercrime includes any criminal or undesired act dealing with mobile devices, computers and networks, also called hacking. Additionally, cybercrime also includes traditional crimes conducted with the help of Internet. A major part of Cyber Security is to fix broken software and to block all loop holes. A major attack vector of Cyber Crime is to exploit broken software and getting access to system through the loop holes. Software security vulnerabilities in cyber space are caused by defective specification, design, and implementation. The generally adopted definition of cybersecurity is the protection of any computer system including mobile devices, software program, and data against unauthorized use, disclosure, transfer, modification, or destruction, whether intentional or accidental. Cyberattacks can be done from internal networks, the Internet, or other private or public systems. Business entities cannot afford to be dismissive of this problem because those who don't respect, address, and counter this as a potential threat will surely become victims. Unfortunately, the current common development practices leave software with many vulnerabilities. To have a secure and reliable cyber infrastructure, the supporting software must contain very few, if any, vulnerabilities [2]. The trend includes exploiting vulnerabilities which go as far back as 2009 in Office documents. Other cross-platform and third-party technologies favored by hackers include Java, Adobe PDF and Adobe Flash. It completely depends on the care that people take followed by the decisions they make when they set up, maintain, and use mobile phones, computers and the Internet. Cyber-security covers both hardware and software protection of personal information and technology resources from unauthorized access gained via technological means. The existing problem of End-User mistakes can't be solved by adding more technology but it has to be solved with a joint effort and partnership between the Information Technology community of interest as well as the general business community along with the critical support of top management and other entities involved. The potential seriousness of Cybercrime is even greater if it affects critical IT systems of telecommunications, power distribution, banking or transport, i.e. of the infrastructure on which virtually most of individual companies depend. Such concerns led the US President to set up a Commission on Critical Infrastructures. However, in this paper we deal

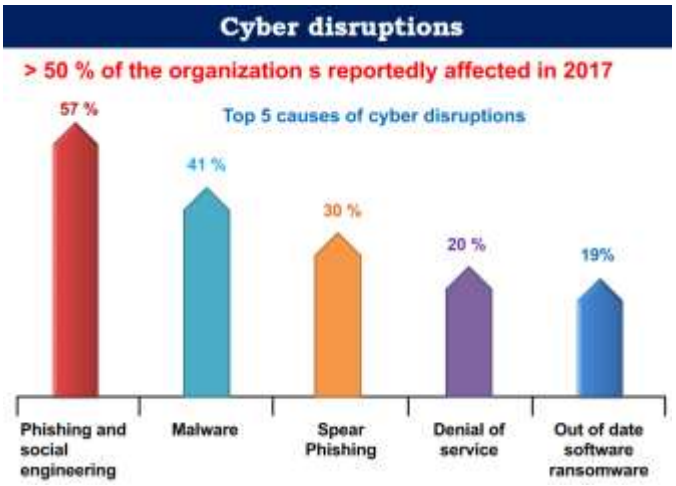

Fig. Cyber Disruptions in India [1]

solely with the defence of corporate IT systems. Such Cybercrimes cannot be considered separately for individual systems, because of the rapidly growing interconnectivity between IT systems, via Intra-nets, Extra-nets and the Internet itself, as well as by direct physical interconnection, or exchangeable storage media such as diskettes. Such interconnectivity (often unintended, rarely adequately planned) turns separate IT systems into components of what is in effect a single large super-system that might suffer an overall failure, or whose data or software may be seriously polluted as a result of a single malicious act or say accident.

1.1 What is Cybersecurity and Cybercrime

Cybersecurity and Cybercrime are two major issues which cannot be separated in an interconnected environment. The fact that the 2010 United Nation's General Assembly resolution on cybersecurity addresses cybercrime as one Major challenge. Cybersecurity plays an important role in the ongoing development of information technology domain, as well as Internet services. Enhancing cybersecurity and protecting critical information infrastructures are essential to every nation's security and economic well-being. Making the cyberspace safer and protecting Internet users across globe has become integral to the development of new services as well as government policy. Preventing cybercrime is an integral component of a national cyber security and critical information infrastructure protection strategy. In particular, this includes the formulation and adoption of appropriate legislation against the misuse of ICTs for criminals or other purposes and other activities that are intended to affect the integrity of national critical infrastructures. At the national level, cybersecurity is a shared responsibility requiring coordinated and strong action related to prevention, preparation, response and recovery from incidents on the part of government authorities, the private sector and citizens of nation. The technical, institutional and legal challenges posed by the issues of cybersecurity are global and have far-reaching consequences, and can only be addressed through a coherent strategy taking into account the role of different involved stakeholders and existing initiatives, within a framework of international cooperation [3].

1.2 Advantages and Risks Associated

The growth of the information society in the world is accompanied by new and serious threats. Essential services like water and electricity supply now rely on ICTs. Vehicles (personal as well as transport), traffic control, elevators, air conditioning and telephones and mobile phones also depend on the smooth functioning of ICTs. Attacks on information infrastructure and Internet services now have the potential to harm society in new and critical ways and will have long lasting impact. Attacks against information infrastructure and Internet services have already taken place in many parts of the world. Online fraud like fishing, trapping, vishing and hacking attacks are just some examples of computer-related crimes that are being committed on a large scale every day. The financial damage caused by cybercrime is reported to be enormous. On the other hand, most of our industrial IT infrastructure is still sufficiently fragmented that there remains a window of opportunity to guide its evolution towards improved security through the progressive introduction of components, such as interface controllers, that provide more effective defence in the face of hostile attack. When properly implemented and managed, such interface controllers (guards, gateways and firewalls) can greatly enhance the security of systems involving the following classes of data flow - particularly where these do not already benefit from end-to-end encryption.

2. THREATS TO CYBER SECURITY

Threats to cybersecurity can be broadly divided into two general categories: actions aimed at and intended to destroy or damage cyber systems and actions that seek to exploit the cyber infrastructure for harmful or unlawful purposes without damaging or compromising that infrastructure—cyber exploitation. While some intrusions may not result in an immediate impact on the operation of a cyber systems, as for example when a —Trojan Horse infiltrates and establishes itself in a computer, such intrusions are considered as cyber-attacks when they can thereafter permit actions that degrade or destroy the

computer's capabilities and capacities. Exploitation of cyberspace includes using the Internet and other cyber systems and tools to commit fraud, to steal, to recruit and train terrorists, to violate copyrights and other rules, limiting the distribution of information, to convey controversial messages (including political and —hated speech), and to sell child pornography or other banned or restricted materials. Following are some new threats to cyberspace. With the rapid increase in the use of free hacking tools and cheap electronic devices such as key loggers and Radio Frequency Scanners, if you use e-mail or your company's systems that are being connected to the Internet, you are being scanned, monitored, probed and attacked constantly. Also, this is true for your vendors and supply chain partners, including payment processors. E-mail and the web are the two main attack vectors used by hackers to infiltrate corporate networks. So, it is clear that every company is vulnerable because every company needs to have these for their functioning. On the other hand, every company required to guard its systems from unwanted and unauthorized access through these openings, it is because supposed firewalls offer no protection whatsoever once a hacker has entered into the system.

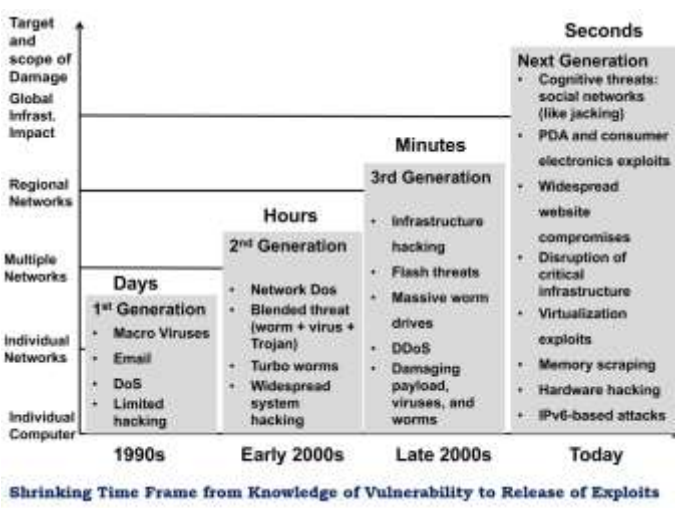

Fig. Time requirement for Exploits [1]

2.1 Development and Design of Tools which automate the Attacks

In the recent time we have seen that software tools are being used to automate attacks. With the help of software and preinstalled attacks, a single offender can attack thousands of computer systems in a single day using one computer. If the offender has access to a greater number of computers – e.g. through a botnet the scale can be increased still further. Since most of such software tools use preset methods of attacks, not all the done attacks prove successful. Individuals who update their operating systems and other software applications on a regular interval reduce their risk of falling victim to these broad-based attacks, as the companies developing protection software analyses attack tools and prepare for the standardized hacking attacks. High-profile attacks are often based on individually-designed attacks.

2.2 Unauthorized Access

Hacking is described as an offence refers to unlawful access to a computer system, one of oldest Computer-based crimes. Following the development of computer networks (mainly the Internet), this crime has become a mass phenomenon. Some famous targets of hacking attacks around the world include the US National Aeronautics and Space Administration (NASA), the US Air Force, the Pentagon, Yahoo, Google, eBay and the German Government, hacking of Bangladeshi Banks, etc. [4]. Examples of such offences include breaking the password of password-protected websites and Circumventing password protection on a computer system. Acts related to the term — hacking does include preparatory acts such as the use of faulty software and/or hardware implementation to illegally obtain a password to enter a computer system, setting up —spoofing websites to make users disclose their Passwords and installing hardware and software-based key logging methods (e.g. —key loggers) that Record every keystroke – and consequently any passwords used on the computer and/or device. Many analysts across globe recognized a rising number of attempts to illegally access computer systems, with over 500 million incidents recorded worldwide during the month of August 2017 alone.

Factors which have backed the fast-increasing number of hacking attacks: rapid development of software tools that automate the attacks, inadequate and incomplete protection of computer systems and the growing role of self-owned private computers as a target of hacking attacks. Interception of communications is normally undetectable and, in the absence of suitable countermeasures, offers a tempting target to attackers. In appropriate computer systems, unauthorized access to data-bases, etc., can be monitored and, where this has been done, it has produced ample evidence that probing attacks are indeed taking place on a substantial and increasing scale. In the current context we regard all attacks which solely seek to gain information, from communications or computers, as —passive.

2.3 Mobile Devices and Applications (Apps)

The exponential growth in mobile devices and its technologies drives an exponential growth in security risks too. Every new smart phone, tablet or other mobile device, opens another window for a cyberattack as each creates another vulnerable access point to networks. This unfortunate dynamic is no longer a secret to thieves who are ready and waiting with heavily targeted malware and attacks employing mobile applications. Similarly, the perennial problem of lost and stolen devices will expand in near future to include these new technologies and old ones that previously flew under the radar of cyber security planning.

2.4 Social Media Networking

Growing use of social media in every corner of world will contribute to personal cyber threats. Adoption of Social Media among businesses is skyrocketing and so is the threat of attack. Institutions can expect to see an increase in social media profiles used as a tool for social engineering tactics. To combat such risks, institutions must need to look beyond the basics of policy and procedure development to more advanced technologies such as data leakage prevention and control, enhanced network monitoring and log file analysis.

2.5 Cloud Computing

More firms will use cloud computing. The cost savings and efficiencies of cloud computing are compelling companies to migrate to the cloud-based services. A well-designed architecture and operational security planning will enable institutions to effectively manage the risks of cloud computing. Unfortunately, current reports and surveys indicate that companies everywhere are underestimating the importance of security due diligence when it comes to vetting these providers. As the use of cloud-based services are rising, new breach incidents will highlight the challenges such services pose to forensic analysis and incident response and the matter of cloud security will finally get its due attention sometimes soon.

2.6 Protect systems rather Information

The primary focus must be on protecting information, and not just systems. As businesses and consumers are likely to move to store more and more of their important information online in cloud-based storage solutions, the requirements for security will go far beyond from simply managing systems to protecting the data these systems house. Rather than focusing on developing processes for protecting the systems that house these information, more granular control will be demanded - by users and by companies - to protect the data stored therein.

2.7 New Platforms and Devices

Newly developed architecture and new devices will create new opportunities for cybercriminals. Security related threats have long been associated with personal computers running Windows but it has changed in last decade. The proliferation of new platforms and new devices - the iPhone, the iPad, Android, for example - created new threats.

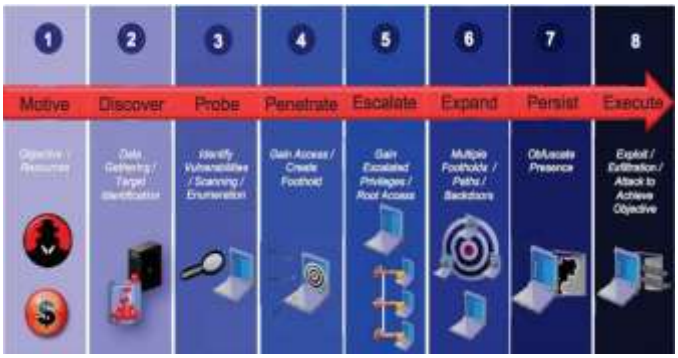

Fig. Phases of Cyberattacks [1]

3. WHAT COULD HAPPEN?

A lot of things: all of them bad. Accordingly, an organization (particularly franchise businesses and other licensors) must evaluate their risk to determine and implement required policies and procedures. We have formulated a —Scale of Cyber in Security, based on the potential harm that might be caused:

1. Low Risk: Hacker has gained access to system but minimally. Minor risk of business disruption, but such access can aid attackers in collective information gathering and planning future attacks.
2. Moderate Risk: Malware has been implanted in the company's network, which could cause mischief and malfunctions. There is a significant risk of a business disruption that could result in great financial loss and/or damage of goodwill.
3. Moderate-to-High Risk: Using sniffers or other equipment, hackers might have obtained personally identifiable information also known as PII from point-of-sale (POS) devices. There is a high risk of a business disruption that could create financial losses and/or damage of goodwill.
4. High Risk: In an organization data is stolen by disgruntled employee. There is a potential risk of

business disruption, resulting in financial loss and damage of goodwill of the organization. PII may be taken, as well as company's confidential information and financial information.

5. Critical Risk: Hackers have gotten into the organization's system and can access PII as well as the organization's financial information and other confidential data. There is a severe risk of business disruption, financial loss, damage of goodwill of organization. Applications, systems and database have been compromised.

4. NECESSITY OF CYBERSECURITY

Data is the most valuable asset with respect to an individual, corporate sector and Government and its authorities. With respect to an individual the concerned areas of focus are:

1. Protecting unauthorized access of data, disclosure, modification of the resources of the system.
2. Security during over the network transactions regarding e-commerce transactions, banking, railway reservations and stock markets.
3. Security of social accounts while using social-networking sites against hijacking.
4. Improved cyber security mechanism and better understanding of the threat and of the vectors used by the attacker to circumvent cyber defenses.
5. Requirement of separate unit handling cyber related security of the organization.
6. Various types of organizations or missions attract different types of adversaries, with different goals, and thus need different levels of preparedness for it.
7. In identifying the nature of the cyber threat an institution faces, the interplay of an adversary's capabilities, intentions and targeting activities must be considered with respect to state and country.
8. Providing security to the information containing various essential surveys and their reports.
9. Securing the data bases and maintaining the details of all the rights of the organizations at various level.

5. SECURITY TRAINING AND AWARENESS

The human factor is the weakest link in any kind of information security program. Communicating the necessity of information security and promoting safe computing are key in securing a company against cybercrime. Following are a few best practices:

1. Use a passphrase that is easy to remember and hard to guess by others like E@tUrVegg1e$ (Eat your veggies) and make sure to use a combination of upper-case and lower-case letters, symbols and numbers to make it less susceptible to brute force and other potential attacks. It is recommended to not to use simple dictionary words as they may subject to dictionary attacks – a type of brute force attack.
2. Do not share or write down any ―passphrases.
3. Communicate/educate your employees and executives on the latest cyber security threats and what they can do to help protect critical information assets.
4. Do not click on links or attachments in e-mail from untrusted sources.
5. Do not send sensitive business files to personal email addresses.
6. Have suspicious/malicious activity reported to security personnel immediately. Secure all network devices when traveling, and report lost or stolen items to the technical support for remote kill/deactivation.
7. Educate employees about phishing attacks and how to report fraudulent activity.

6. CONCLUSIONS

This paper has explored and examined the significance of privacy for individuals as a fundamental human right. Human rights violations arise from the unlawful collection and storage of personal data, or the abuse, the problems associated with inaccurate personal data, or unauthorized disclosure of such data, etc. In this paper we also include the current problems, threats, issues, challenges and measures of Information Technology sector in our society. With the increasing incidents of cyber-attacks, building an effective intrusion detection model with good accuracy and real-time performance are essential. The Cybercrime as a whole refers to unlawful behavior that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause mental or physical harm to the victim indirectly or directly, using modern telecommunication ways such as Internet and mobile phones (Fake calls/SMS/MMS)".

Crimes like this may threatens the nation's security and financial health. Issues of this type have become high-profile, particularly those surrounding cracking, hacking, spoofing, skimming, copyright infringement, child pornography, and child grooming. Also, there are problems of privacy when confidential and important information is lost or intercepted, lawfully or otherwise. A computer or other network device can be a source of evidence. Even then when a computer is not directly used for criminal activities, may contain records of value to criminal investigators, so the network must be secure as no one can access the information of the computer. The potential risks of cyber-crime are very real and too threatening to be ignored. Every licensor and franchisor, indeed every business/institution owner, has to face up to

their vulnerability and do something about it. At the very least, every company must conduct a professional assessment i.e. audit of their cyber security and cyber risk; engage in a prophylactic plan to minimize the liability; insure safety against losses to the greatest extent possible; and promote and implement a well-thought out cyber policy and regulations, including crisis management in the event of a worst case scenario.

ACKNOWLEDGEMENT

We would like to express our gratitude towards our University, Dr A. P. J. Abdul Kalam Technical University for adopting Cybersecurity as subject in Engineering Courses this enables us to understand the depth and importance of subject. Also, we would like to thank our institution ABES Engineering College, Ghaziabad for their kind support and guidance in our work.
Finally, we must express our very profound gratitude to our parents for providing us with unfailing support and continuous encouragement throughout, this achievement would not have been possible without them.

REFERENCES

[1] Dr V. K. Saraswat, "Conference on Cybersecurity by NITI Aayog at Vigyan Bhawan Delhi, 2018".

[2] Moore, R. (2005) "Cybercrime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing

[3] Guinier D, Dispositif de gestion de continuité – PRA/PCA: une obligation légale pour certainset un impératif pour tous (Continuity Planning – BRP/BCP: a legal requirement for some and a vital necessity for all). Expertises, no. 308, Nov. 2006, pp. 390 -396.

[4] CSIS: Securing Cyberspace for the 44th Presidency, CSIS Commission on Cybersecurity, US Center for Strategic and International Studies (CSIS), Washington DC, December 2008.