A Study of Cyber Security Trends and Its Challenges: A Conceptual Framework

Nivedita Singh
(Student, M. Tech., Bharat Institute of Technology, India)

Abstract

Cyber Security plays a vital role within the field of information technology .Securing the information became one in every of the most important challenges within the present day. once ever we predict concerning the cyber security the primary factor that comes to our mind is 'cyber crimes' that are increasing immensely day by day. Numerous Governments and firms area unit taking several measures so as to forestall these cyber crimes. Besides numerousmeasures cyber security continues to be a really huge concern to several. This paper primarily focuses on challenges long-faced by cyber security on the newest technologies .It additionally focuses on latest concerningthe cyber security techniques, ethics and therefore the trends ever-changing the face of cyber security.

Cybersecurity may be a necessary thought for info technology still as net services. we want to acknowledge the importance of various sorts of risks that exist within the on-line world Enhancing cyber security and protectiveessential info area unit essential to nation's security and economic being. Whenever we expect concerning the cyber security we expect - taking several measures to stop the cyber-crime. This paper primarily focuses on trends, challenges and cyber ethics within the field of cyber security. Cyber incidents emphasize the importance of staying up-to-date on world cybercrime trends, particularly regarding the utilization of mobile and privatecomputing devices.

Keywords: *cyber security, cyber-crime, cyber ethics, social media, cloud computing*

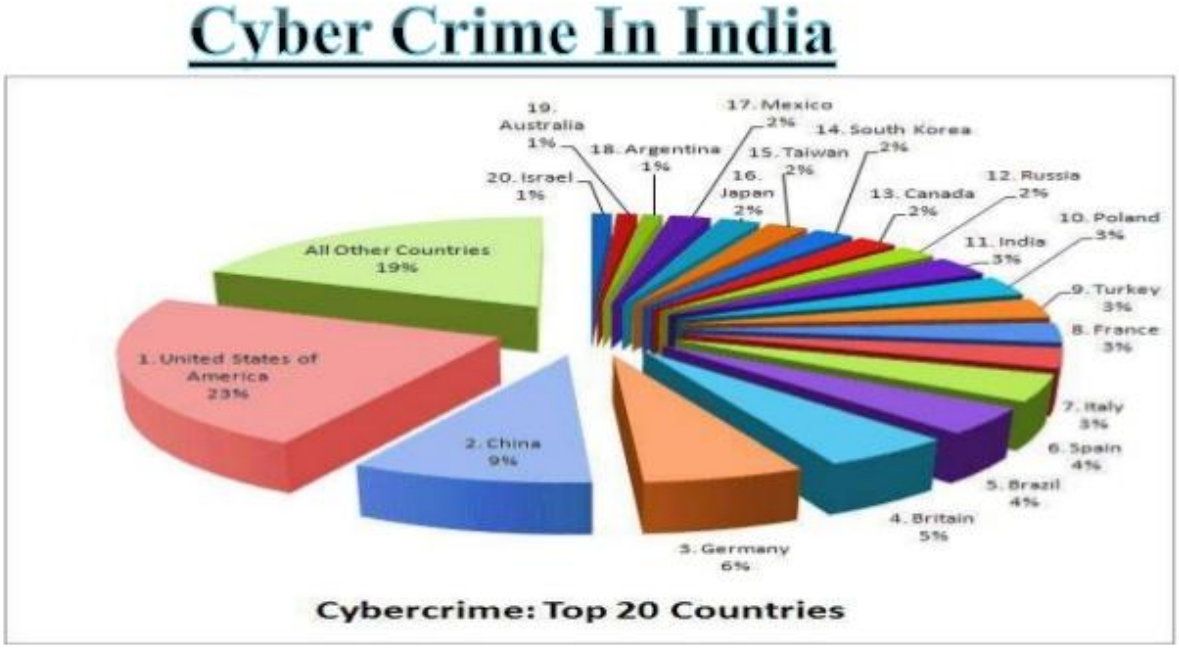
1.INTRODUCTION

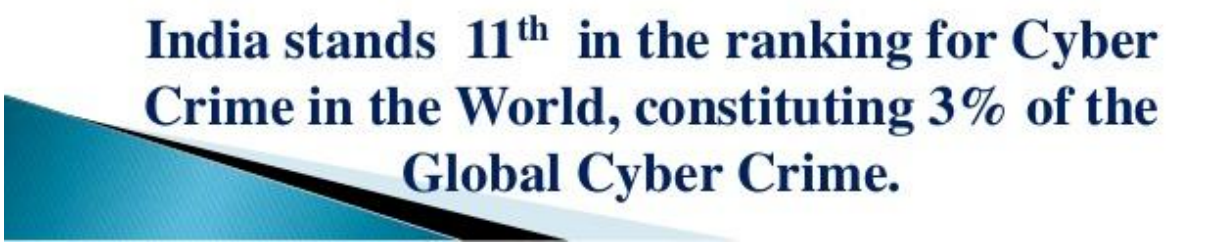
Today man is ready to send and receive any kind of information is also an e-mail or an audio or video simply by the press of a howeverton but did he ever suppose however firmly his information id being transmitted or sent to the opposite person safely without any outflow of information?? the solution lies in cyber security. nowadays internetis that the quickest growing infrastructure in a day life. In today's technical surroundings several latest technologies area unit ever-changing the face of the person kind. however thanks to these rising technologies we have a tendency to area unit unable to safeguard our personal info terribly} very effective means and thuscurrently cyber crimes area unit increasing day by

day. nowadays over sixty p.c of total industrial transactions area unit done on-line, therefore this field needed a top quality of security for clear and best transactions. thus cyber security has become a modern issue. The scope of cyber security isn't simply restricted to securing the data in IT trade however additionally to varied alternative fields like cyber area etc. Even the most recent technologies like cloud computing, mobile computing, E-commerce, web banking etc additionally desires high level of security. Since these technologies hold some vital info relating to an individual their security has become a requirementissue. Enhancing cyber security and protective crucial info infrastructures are essential to every nation's security and economic welfare. creating the net safer (and protective net users) has become integral to the event of recentservices still as governmental policy. The fight against cyber crime desires a comprehensive and a safer approach. as long as technical measures alone cannot stop any crime, it's essential that enforcement agencies are allowed to analyze and prosecute cyber crime effectively. nowadays several nations and governments are imposing strict laws on cyber securities so as to forestall the loss of some vital info. each individual should even be trained on this cyber security and save themselves from these increasing cyber crimes

CYBERCRIME

Cyber crime may be a term for any criminality that uses a laptop as its primary suggests that of commission and thieving. The U.S. Department of Justice expands the definition of cyber crime to incorporate any criminality that uses a laptop for the storage of proof. The growing list of cyber crimes includes crimes that are created potentialby computers, like network intrusions and therefore the dissemination of laptop viruses, still as computer-based variations of existing crimes, like fraud, stalking, bullying and act of terrorism that became as major drawback to individuals and nations. sometimes in common man's language cyber crime is also outlined as crime committed employing a laptop and therefore the net to steel a person's identity or sell contraband or stalk victims or disrupt operations with malevolent programs. As day by day technology is enjoying in major role during a person's life the cyber crimes additionally can increase beside the technological advances.



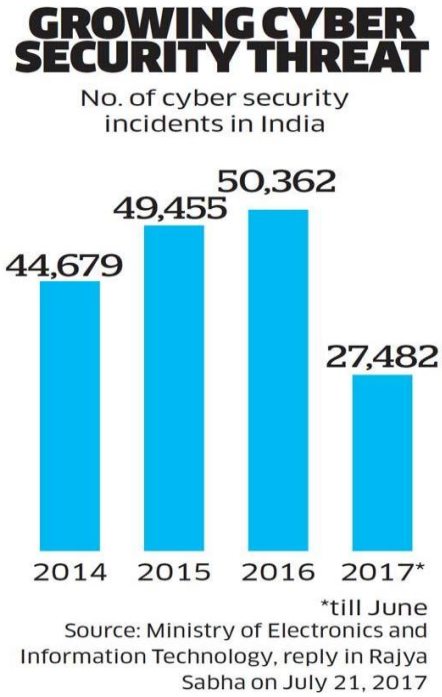


https://www.google.com/search?q=latest+data+of+cyber+crime+in+india&tbm=isch&tbs=rimg:Cfp8fiGq4JMfIjgCD1_18T0InRfpnz-LuVnNWOus5f2LxdHT1vZ2NnyCb6Xdz9x-_1Aua7KB3msztitrx43-Bm8QbzXSoSCQIPX_1xPQidFEdmnSoz2iR_1kKhIJ-mfP4u5Wc1YR7BgKmYHDiYcqEgk66zl_1YvF0dBEx1p4FMogXNioSCfW9nY2fIJvpEfxpFQ2iD0VyKhIJd3P3H78C5rsRqJJBLh0cZSIqEgkoHeazO2K2vBFrFhe33ii06CoSCXjf4GbxBvNdETR8FH2IHMJW&tbo=u&sa=X&ved=2ahUKEwjd3N3rrZDgAhUZb30KHXaQBAkQ9C96BAgBEBg&biw=1366&bih=608&dpr=1#imgdii=XauA3XlijGYpcM:&imgrc=KMjzlzrqLdPNZM

The Concept of Cybersecurity

Over the past several years, experts and policymakers have expressed increasing concerns about protecting ICT systems from cyberattacks—deliberate attempts by unauthorized persons to access ICT systems, usually with the goal of theft, disruption, damage, or other unlawful actions. Many experts expect the number and severity of cyberattacks to increase over the next several years. The act of protecting ICT systems and their contents has come to be known as cybersecurity. A broad and arguably somewhat fuzzy concept, cybersecurity can be a useful term but tends to defy precise definition. It usually refers to one or more of three things: A set of activities and other measures intended to protect—from attack, disruption, or other threats—computers, computer networks, related hardware and devices software and the information they contain and communicate, including software and data, as well as other elements of cyberspace.The state or quality of being protected from such threats.

The broad field of endeavor aimed at implementing and improving those activities and quality.



Source: https://economictimes.indiatimes.com/tech/internet/india-as-vulnerable-as-any-other-country-in-the-world-eugene-kaspersky/articleshow/62224333.cms

The Concept of Cyber Security

Over the past many years, specialists and policymakers have expressed increasing issues regarding protective ICT systems from cyberattacks—deliberate tries by unauthorized persons to access ICT systems, sometimes with the goal of stealing, disruption, damage, or different unlawful actions. Several specialists expect the quantity and severity of cyberattacks to extend over ensuing many years. The act of protective ICT systems and their contents has return to be referred to as cybersecurity.

A broad and arguably somewhat fuzzy construct, cybersecurity is a helpful term however tends to defy precise definition. it always refers to 1 or additional of 3 things: a collection of activities and different measures meant to protect—from attack, disruption, or different threats—computers, laptop networks, connected hardware and devices computer code and also the data they contain and communicate, together with computer code and information, likewise as different parts of computer network.The state or quality of being shielded from such threats.

The broad field of endeavor aimed toward implementing and rising those activities and quality.

CYBERSECURITY

Privacy and security of the info can continuously be prime security measures that any organization takes care. we tend to are presently living in an

exceedingly world wherever all the data is maintained in an exceedingly digital or a cyber type. Social networking sites give an area wherever users feel safe as they move with friends and family. within the case of home users, cyber-criminals would still target social media sites to steal personal information. Not solely social networking however additionally throughout bank transactions an individual should take all the specified security measures.

There will be new attacks on automaton software system based mostly devices, however it'll not get on hugescale. the actual fact tablets share a similar software system as good phones suggests that they're going to be shortly targeted by a similar malware as those platforms. the quantity of malware specimens for Macs would stillgrow, though a lot of but within the case of PCs. Windows eight can enable users to develop applications for just about any device (PCs, tablets and good phones) running Windows eight, thus it'll be potential to develop malicious applications like those for android, therefore these square measure a number of the anticipated trends in cyber security

Company Name	What Happened
Reliance Jio	Unauthorised access into a part of database
Star	Unreleased episodes of Games of Thrones leaked
Union Bank	Hackers managed to steal Union Bank's access codes for the Society for Worldwide Interbank Financial Telecommunication (SWIFT).
Axis Bank	Unauthorized login by an unnamed, offshore hacker.
Zomato	17 million user records from its database were hacked.
Renault India	Hit by Ransomware Wannacry in global attack
IRCTC	Data theft from website
Yes Bank	Malware attacked some ATMs and POS machines
Hitachi Payment Systems	Malware caused breach of bank data
Bank of Maharashtra	central server hacked
Reckitt Benckiser India	Hit by global ransomware attack

Source: https://economictimes.indiatimes.com/tech/internet/how-india-inc-is-losing-its-cybersecurity-war/articleshow/61074845.cms

Management of Cyber security

Risks The risks related to any attack rely on 3 factors: threats (who is attacking), vulnerabilities (the weaknesses they're attacking), and impacts (what the attack does). The management of risk to data systems is taken into account basic to effective cybersecurity.

What are the Threats?

People WHO truly or probably perform cyberattacks are wide cited as falling into one or a lot of of 5 categories: criminals out to financial gain from crimes like theft or extortion; spies out to stealing classified or proprietary data employed by government or personal entities; nation-state warriors WHO develop capabilities and undertake cyberattacks in support of a country's strategic objectives; "hacktivists" WHO perform cyberattacks for nonmonetary reasons; and terrorists who interact in cyberattacks as a sort of non-state or state-sponsored warfare.

What are the Vulnerabilities?

Cybersecurity is in many ways an race between attackers and defenders. ICT systems are very complicated, and attackers are perpetually looking for weaknesses, which may occur at several points. Defenders will usually defend against weaknesses, however 3 are significantly challenging: unintended or intentional acts by insiders with access to a system; offer chain vulnerabilities, which may allow the insertion of malicious computer code or hardware throughout the acquisition process; and previously unknown, or zero-day, vulnerabilities with no established fix. Even for vulnerabilities wherever remedies ar familiar, they'll not be enforced in several cases owing to fund or operational constraints.

What are the Impacts?

A fortunate attack will compromise the confidentiality, integrity, and availability of an ICT system and therefore the data it handles. Cybertheft or cyberespionage may result in exfiltration of monetary, proprietary, or personal data from that the wrongdoer will profit, usually without the knowledge of the victim. Denial-of-service attacks will slow or stop legitimate users from accessing a system. Botnet malware will provide an offender command of a system to be used in cyberattacks on alternative systems. Attacks on industrial management systems may result within the destruction or disruption of the instrumentality they management, like generators, pumps, and centrifuges.

Most cyberattacks have restricted impacts, however a successful attack on some elements of important infrastructure (CI)—most of that is control by the personal sector—could have important effects on national security, the economy, and therefore the support and safety of individual voters. Thus, a rare fortunate attack with high impact will create a bigger risk than a typical successful attack with low impact.

While it's well known that cyberattacks will be expensive to people and organizations, economic impacts will be troublesome to live, and estimates of these impacts vary wide. associate degree usually cited figure for annual value to the worldwide economy from law-breaking is $400 billion, with some observers difference that prices are increasing well, particularly with the continuing growth of ICT infrastructure through the net of Things and different new and rising platforms.6 the prices of cyberespionage will be even tougher to quantify however are thought-about to be substantial.7

Managing the risks from cyberattacks sometimes involves (1) removing the threat supply (e.g., by closing down botnets or reducing incentives for cybercriminals); (2) addressing vulnerabilities by hardening ICT assets (e.g., by fixing computer code and training

employees); and (3) drop-off impacts by mitigating harm and restoring functions (e.g., by having back-up resources out there for continuity of operations in response to associate degree attack). The optimum level of risk reduction can vary among sectors and organizations. for instance, the extent of cybersecurity that customers expect could also be lower for a corporation within the diversion sector than for a bank, a hospital, or a government agency.

Trends Chanbging Cyber Security

Here mentioned below are a number of the trends that are having an enormous impact on cyber security.

Web servers:

The threat of attacks on web applications to extract information or to distribute malicious code persists. Cyber criminals distribute their malicious code via legitimate net servers they've compromised. however data-stealing attacks, several of that get the eye of media, also are an enormous threat. Now, we'd like a larger emphasis on protective net servers and net applications. net servers are particularly the best platform for these cyber criminals to steal the information. thence one should always use a safer browser particularly throughout vital transactions so as to not fall as a prey for these crimes.

Cloud computing and its services

These days all little, medium and enormous companies are slowly adopting cloud services. In alternative words the planet is slowly moving towards the clouds. This latest trend presents an enormous challenge for cyber security, as traffic will go around traditional points of scrutiny. additionally, because the variety of applications offered within the cloud grows, policy controls for net applications and cloud services will ought to evolve so as to stop the loss of valuable info. although cloud services are developing their own models still loads of problems ar being remarked regarding their security. Cloud could offer huge opportunities however it should be noted that because the cloud evolves thus as its security concerns increase.

APT's and targeted attacks

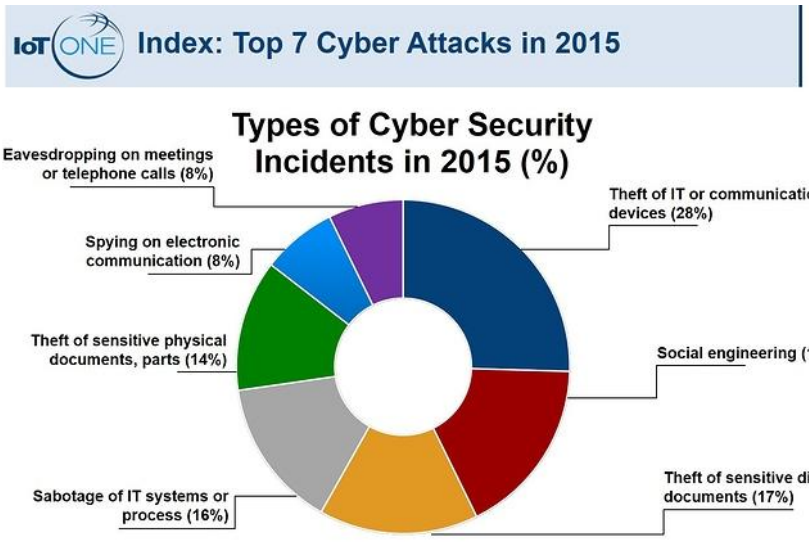
APT (Advanced Persistent Threat) may be a whole new level of cyber crime ware. For years network security capabilities like net filtering or IPS have contend a key half in distinguishing such targeted attacks (mostly once the initial compromise). As attackers grow bolder and use additional imprecise techniques, network security should integrate with alternative security services so as to observe attacks. thence one should improve our security techniques so as to stop a lot of threats coming within the future.

Mobile Networks

Today we are able to connect with anyone in any a part of the globe. but for these mobile networks security may be a terribly massive concern. currently firewalls and different security measures are getting porous as individuals ar using devices like tablets, phones, PC's etc all of that again need further securities aside from those gift within the applications used. we have a tendency to should always believe the protection problems with these mobile networks. additional mobile networks ar extremely liable to these cyber crimes a lot of care should be taken just in case of their security problems.

IPv6:

New net protocol IPv6 is that the new net protocol that is replacing IPv4 (the older version), that has been a backbone of our networks generally and also the net at massive. protective IPv6 isn't simply a matter of porting IPv4 capabilities. whereas ipv6 may be a wholesale replacement in creating a lot of IP addresses offered, there are some very elementary changes to the protocol which require to be thought-about in security policy. thence it's invariably higher to change to IPv6 as soon as potential so as to reduce the risks concerning cyber crime. 4.6 secret writing of the code encryption is that the method of coding messages (or information) in such the simplest way that eavesdroppers or hackers cannot browse it.. In AN encryption scheme, the message or info is encrypted exploitation AN cryptography algorithmic program, turning it into AN unclear cipher text. this is often sometimes done with the utilization of AN cryptography key, that specifies however the message is to be encoded. encryption at a awfully starting level protects information privacy and its integrity. however additional use of encryption brings additional challenges in cyber security. encryption is additionally used to defend information in transit, for instance information being transferred via networks (e.g. the net, ecommerce), mobile telephones, wireless microphones, wireless intercoms etc. thence by encrypting the code one will understand if there's any outflow of knowledge. thence the higher than are a number of the trends dynamical the face of cyber security within the world. the highest network threats are mentioned in below



Source:https://community.iotone.com/t/iot-one-index-top-7-cyber-attacks-in-2015/47

ROLE OF SOCIAL MEDIA IN CYBER SECURITY

As we tend to become additional social in an progressively connected world, firms should realize new ways in which to safeguard personal data. Social media plays an enormous role in cyber security and can contribute a lot to non-public cyber threats. Social media adoption among personnel is skyrocketing so is that the threat of attack. Since social media or social networking sites are almost utilized by most of them on a daily basis it's become an enormous platform for the cyber criminals for hacking non-public data and stealing valuable information. in a very world wherever we're fast to offer up our personal data, firms have to ensure they're even as fast in distinctive threats, responding in real time, and avoiding a

breach of any kind. Since individuals are simply attracted by these social media the hackers use them as a bait to urge {the information|the knowledge|the information} and also the data they need. therefore folks should take applicable measures particularly in handling social media so as to stop the loss of their data. the flexibility of people to share data with AN audience of millions is at the center of the actual challenge that social media presents to businesses. additionally to giving anyone the facility to propagate commercially sensitive data, social media conjointly provides constant power to spread false data, which may be simply being as damaging. The speedy unfold of false data through social media is among the rising risks known in world Risks 2013 report. although social media is used for cyber crimes these firms cannot afford to prevent exploitation social media because it plays a crucial role in content of an organization. Instead, they need to have solutions that may apprise them of the threat so as to repair it before any real injury is finished. but firms ought to perceive this and recognise the importance of analysing the knowledge particularly in social conversations and provide acceptable security solutions so as to remain aloof from risks. One should handle social media by exploitation sure policies and right technologies.

CYBER SECURITY TECHNIQUES

Access control and password security

The conception of user name and password has been basic approach of protective our data. this could be one amongst the primary measures relating to cyber security.

Authentication of data

The documents that we tend to receive should be genuine be before downloading that's it ought to be checked if it's originated from a trustworthy and a reliable source which they're not altered. Authenticating of those documents is sometimes done by the opposing virus code gift within the devices. so an honest opposing virus code is additionally essential to guard the devices from viruses.

Malware scanners

this is often software that sometimes scans all the files and documents present in the system for malicious code or harmful viruses. Viruses, worms, and Trojan horses area unit samples of malicious code that area unit usually classified together and referred to as malware.

Firewalls

A firewall may be a software program or piece of hardware that helps classify hackers, viruses, and worms that attempt to reach your pc over the net. All messages getting into or going away the net go through the firewall present, that examines every message and blocks people who don't meet the required security criteria. hence firewalls play a very important role in detective work the malware.

Anti-virus software

Antivirus software may be a computer program that detects, prevents, and takes action to disarm or take away malicious computer code programs, like viruses and worms. Most associate degreetivirus programs include an auto-update feature that allows the program to transfer profiles of recent viruses so it will check for the new viruses as shortly as they're discovered. an anti virus software is a must and basic necessity for each system. **RECENT SURVEY PROBLEMS ON CYBER SECURITY TRENDS**

The following list was developed from cyber security analysis and survey

Mobile Devices and Apps

The exponential growth of mobile devices drives an exponential growth in security risks. each new smart phone, tablet or different mobile device, opens another window for a cyber attack, as every creates another vulnerable access point to networks. This unfortunate dynamic is not any secret to thieves who are prepared and waiting with extremely targeted malware and attacks using mobile applications. Similarly, the perennial downside of lost and stolen devices can expand to incorporate these new technologies and previous ones that previously flew under the radar of cyber security designing.

Social Media Networking

Growing use of soc media can contribute to private cyber threats. Social media adoption among businesses is skyrocketing then is that the threat of attack. In 2012, organizations will expect to ascertain a rise in social media profiles used as a channel for social engineering ways. To combat the risks, firms can ought to look on the far side the fundamentals of policy and procedure development to additional advanced technologies like information outflow prevention, increased network observation and log file analysis.

Cloud Computing

Additional companies can use cloud computing. the numerous value savings and efficiencies of cloud computing square measure compelling firms to migrate to the cloud. A elegant design and operational security designing can alter organizations to effectively manage the risks of cloud computing. sadly, current surveys and reports indicate that firms are underestimating the importance of security due diligence once it involves vetting these suppliers. As cloud use rises in 2012, new breach incidents can highlight the challenges these services cause to forensic analysis and incident response and also the matter of cloud security can finally get its due attention.

Protect systems rather info

The stress are on protective info, not simply systems. As customers and businesses square measure like move to store additional and additional of their vital info on-line, the wants for security can go beyond merely managing systems to protective the info these systems house. instead of that specialize in developing processes for safeguarding the systems that house info, additional granular management are demanded - by users and by firms - to guard the info stored therein.

New Platforms and Devices

New platforms and new devices can produce new opportunities for cybercriminals. Security threats have long been related to personal computers running Windows. however the proliferation of recent platforms and new devices - the iPhone, the iPad, Android, for instance - can probably produce new threats. The android phone saw its initial Trojan this summer, and reports continue with malicious apps and spyware, and not simply on mechanical man.

Everything Physical will be Digital

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

Long-Term Challenges

The legislative and executive-branch actions discussed above are mostly designed to address many well-established near-term needs in cybersecurity: preventing cyber-based disasters and undercover work, reducing impacts of successful attacks, rising inter- and intrasector collaboration, informative federal agency roles and responsibilities, and fighting law-breaking. However, those desires exist within the context of harder long challenges concerning style, incentives, consensus, and environment (DICE):

Design:

Experts typically say that effective security must be an integral a part of ICT style. Yet, developers have historically focused additional on options than security, for economic reasons. Also, several future security needs can not be foreseen, posing a tough challenge for designers.

Incentives:

The structure of economic incentives for cybersecurity has been known as distorted or maybe perverse. cybercrime is thought to be low-cost, profitable, and relatively safe for the criminals. In distinction, cybersecurity will be costly, is by its nature imperfect, and also the economic returns on investments are typically unsure.

Consensus:

Cybersecurity means that various things to totally different stakeholders, usually with very little common agreement on meaning, implementation, and risks. Substantial cultural impediments to consensus also exist, not solely between sectors however among sectors and even among organizations. ancient approaches to security is also short within the hyperconnected environment of cyberspace, however accord on alternatives has well-tried elusive.

Environment:

computer network has been known as the quickest evolving technology area in human history, each in scale and properties. New and rising properties and applications—especially social media, mobile computing, big data, cloud computing, and also the net of Things—further complicate the evolving threat atmosphere, however they will additionally create potential opportunities for rising cybersecurity, as an example through the economies of scale provided by cloud computing and massive information analytics. Legislation and executive actions within the 114th and future Congresses may have important impacts on those challenges. as an example, cybersecurity R&D could have an effect on the design of ICT, cybercrime penalties could influence the structure of incentives, the authority framework could facilitate action of a accord on cybersecurity, and federal initiatives in cloud computing and alternative new elements of computer network could facilitate shape the evolution of cybersecurity

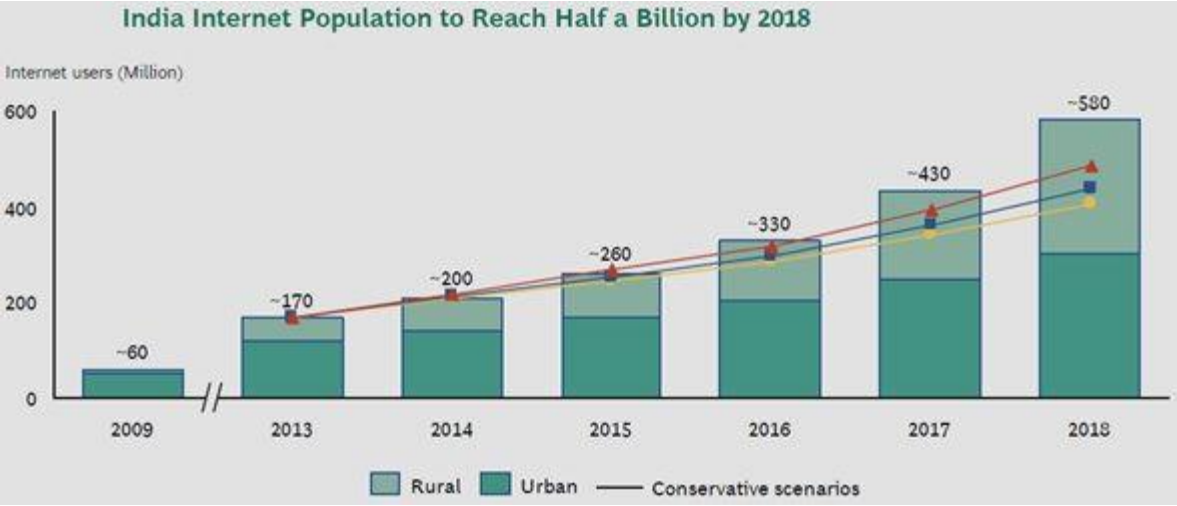
PRACTICES AND CONCERN BY GOVERNMENTS FOR CYBER SECURITY

Ensure that national cyber security policies include the needs of all citizens and not simply central government facilities. Encourage the widespread commendation and use of the cybercrime Convention and different potential international treaties. Support end-user education as this advantages not only the individual user and system however reduces the numbers of unprotected computers that area unit on the market for hijacking by criminals then used to mount attacks.

Use acquisition power, standards-setting and licensing to influence industry suppliers to supply properly tested hardware and software. Extend the development of specialist police and forensic computing resources. Support the international laptop Emergency Response Team (CERT) community, including through funding, because the possibly means that by which a large-scale net drawback are often averted or mitigated . Fund research into such areas as: strong net protocols, Risk Analysis, Contingency coming up with and Disaster Propagation Analysis, Human Factors within the use of laptop systems, Security economic science [16].

KEY CHALLENGES TO SOCIETY

Our Nation's vital infrastructures are composed of public and personal institutions within the sectors of public health, emergency services, government, defense industrial base, data and telecommunications, energy, transportation, banking and finance. India's reliance on technology also reflects from the very fact that India is shifting gears by moving into facets of e-governance. India has already brought sectors like taxation, passports visa under the realm of e - governance. Sectors like police and judiciary are to follow. The travel sector is additionally heavily reliant on this. Most of the Indian banks have gone on complete computerization. This has also brought in ideas of e-commerce and e-banking. The stock markets have also not remained immune [1].



Source: https://www.mbaskool.com/business-articles/operations/14005-digital-india-and-cyber-security-industry.html

CONCLUSION

Cyber crime is now serious, widespread, aggressive, growing, and increasingly sophisticated, and poses major implications for national and economic security. Many industries, institutions, public- and private-sector organizations (particularly those within the critical infrastructure) are at significant risk. For businesses and governments alike, getting the Cyber Security posture right across all its elements will be vital for future growth, innovation and competitive advantage. There is no single answer for success, but by working across public and private sector partnerships and by advancing security measures particularly with regard to mission-critical systems, processes and applications that are connected into cyberspace, businesses will be able to work towards a future environment Fig. 3 that is both open and secure and prosperous.

Cyber crime is currently serious, widespread, aggressive, growing, and more and more refined, and poses major implications for national and economic security. several industries, institutions, public- and private-sector organizations (particularly those inside the vital infrastructure) are at vital risk. For businesses and governments alike, obtaining the Cyber Security posture right across all its components are going to be important for future growth, innovation and competitive advantage. there's no single answer for success, however by working across public and personal sector partnerships and by advancing security measures significantly with relation to mission-critical systems, processes and applications that area unit connected into Net, businesses are going to be able to work towards a future atmosphere Fig. three that's each open and secure and prosperous.

REFERENCES

- *See, for example, Lee Rainie, Janna Anderson, and Jennifer Connolly, Cyber Attacks Likely to Increase (Pew Research Internet Project, October 2014), http://www.pewInternet.org/2014/10/29/cyber-attacks-likely-to-increase/.*
- *The term cyberspace usually refers to the worldwide collection of connected ICT components, the information that is stored in and flows through those components, and the ways that information is structured and processed.*
- *For a more in-depth discussion of this concept, see CRS Report RL32777, Creating a National Framework for Cybersecurity: An Analysis of Issues and Options, by Eric A. Fischer.*
- *See, for example, Department of Homeland Security, "Continuous Diagnostics and Mitigation (CDM)," June 24, 2014, http://www.dhs.gov/cdm.*
- *See, for example, National Institute of Standards and Technology, Managing Information Security Risk: Organization, Mission, and Information System View, March 2011, http://csrc.nist.gov/publications/nistpubs/800-39/ SP800-39-final.pdf.*
- *See, for example, Center for Strategic and International Studies, "Net Losses: Estimating the Global Cost of Cybercrime" (McAfee, June 2014), http://www.mcafee.com/us/resources/reports/rp-economic-impactcybercrime2.pdf?cid=BHP028; Cybersecurity Ventures, "Cybersecurity Market Report, Q2 2016," 2016, http://cybersecurityventures.com/cybersecurity-market-report/. For more information on the Internet of Things, see CRS Report R44227, The Internet of Things: Frequently Asked Questions, by Eric A. Fischer.*

- *Office of the National Counterintelligence Executive, "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011," October 2011, https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/20111103_report_fecie.pdf.*
- *Integrated Defense Staff, "National Informatics Center", Ministry of Defense, India*
- *Yang, Miao, "ACM International Conference Proceeding Series", vol. 113*
- *Unisys Corporation, "Unisys Descriptive Technology & Trends Points of White Paper Series- Cyber Security" USA, 2011*
- *Cyber Security Strategy of United Kingdom, 2009*
- *ITU Cyber Security Work Program to Assist Development Countries, 2009*
- *Rev. Jonames Burg, TTU WTSA Resolution 50, 2008*
- *ITU Cyber Security Work Program to Assist Development Countries, 2008*
- *Kellermann, "Technology Risk Checklist, Cybercrime and Security", IIB-2*
- *Schjolberg/Hubbard, "Harmonizing National Legal Approaches on Cybercrime", 2005*
- *The most Important Instruments in fight against Cybercrime, Ch. 6.2*
- *Luis Corrons, Technical Director, Panda Labs, Bangalore, 2012*
- *Arun Prabhudesai, "Cyber Attacks In India", 2011*
- *Audry Watters, Read Write Cloud, RWW Solution Series, 2010*
- *Amichai Shulan, Application Defense Center (ADC), Amicha Regularly Lactures, Security, 2011*
- *Allen and Hamilton, Reports, "Top Ten Cyber Security Trends for Financial Services", 2012*
- *Peter Sommer, Ian Brown, OECO Project, "Reducing Systemic Cyber Security Risk", 2011 Figure taken from Google images. [18] Ammal Security Report, Panda Labs, 2011*
- *A Sophos Article 04.12v1.dNA, eight trends changing network security by James Lyne.*
- *Cyber Security: Understanding Cyber Crimes- Sunit Belapure Nina Godbole*
- *Computer Security Practices in Non Profit Organisations – A NetAction Report by Audrie Krause.*
- *A Look back on Cyber Security 2012 by Luis corrons – Panda Labs.*
- *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*
- *IEEE Security and Privacy Magazine – IEEECS "Safety Critical Systems – Next Generation "July/ Aug 2013.*
- *CIO Asia, September 3rd , H1 2013: Cyber security in malasia by Avanthi Kumar.*