The Reality of Technologies for Cyber Security Challenges

Hena Iqbal, Ghassan Al-Utaibi, Om Prakash Bohra

Abstract:In the field of informational technology, cyber securit y plays an important role in ensuring that information has becom e one of today's major challenges. The first thing that comes to our mind when we ever talk about cyber security is ' cyber crimes, ' which are rising exponentially every day. Different governments and companies take numerous measures to prevent such cyber crimes. In addition to various cyber security measures, many still have a major concern. It also reports on the innovations in cyber security strategies, practices and developments that change the face of online health. This paper focuses mainly on cyber security challenges facing the latest technologies.

Keywords: Web safety, internet crime, cyber ethics, social networking, smartphone devices, cloud computing

I. INTRODUCTION

Man can today send and receive any form of data, whethe r email, audio or video by simply pressing the button, but ha s he ever considered how securely he can transmit or send hi s data I d securely without any information leakage to anoth er person? The solution is cyber-safety. The Internet today is the most rapidly expanding infrastructure in daily life. Several latest technologies are changing the face of the human race in today's technological climate. But as we are unable to protect our private information in a very effective way due to these emerging technologies, cyber crimes are increasing very fast. Today, more than 60 per cent of all commercial transactions are carried out electronically, demanding a high level of security for secure and better transactions.

Cyber security has therefore become a new problem. Cyber security is not only a question of protecting knowledge in the IT field, but also for certain industries like cyberspace and more. Also, high security is required for even the latest technologies, like cloud, mobile computing, e-commerce, net banking etc. Since these technologies contain important information about a person, their safety is a must. Improvement of cyber security and protection of critical information infrastructures are vital to the safety and economic well-being of each nation. The safeguarding (and safety of internet users) of the Internet has become an essential aspect in the development of new technology and public policies. Cyber crime must be combated in a comprehensive and secure way.

Revised Manuscript Received on April 15, 2020.
*** Correspondence Author**
Dr. Hena Iqbal*, School of Engineering and IT Al Dar University College, Al Garhoud, Dubai, UAE, Email: hena@aldar.ac.ae
Ghassan Al-Utaibi, School of Business, Al Dar University College, Al Garhoud, Dubai, UAE, Email: ghassanalutaibi@aldar.ac.ae
Om Prakash Bohra, School of Business, Al Dar University College, Al Garhoud, Dubai, UAE, Email: bohra@aldar.ac.ae

As technical measures alone cannot prevent crimes, the effective investigation and prosecution of cyber crime by law enforcement agencies is critical. In order to prevent the loss of important information, many nations and governments are currently imposing strict laws on cyber securities. Everyone must also be trained in cyber safety and be free of the growing cybercrimes.

A. Recent Survey on Cyber Crime:

The exponential growth in mobile devices leads to an exponential growth in security risks. Cyber security risks are growing exponentially. Through new Smartphone, laptop or other mobile device creates another cyber attack portal, each of which providing another insecure network access point. This grim paradigm is no mystery to thieves who wait and are ready with targeted ransomware and attacks utilizing mobile apps The ongoing issue of missing and compromised computers will also be broadened to include these new and old innovations, which were once part of cyber-security expected radar.

B. Social Media Networking :

The expanded use of social media would support specific cyber threats. The use of social media by businesses is skyrocketing and thus the threat of attack. Organizations anticipate the social media profiles to increase as a platform for strategies in social engineering in 2012. To counter the threats, organizations need to consider increasingly advanced technologies such as data leakage protection, improved network monitoring and log file review beyond the fundamentals of regulation and procedural growth.

C. Cloud Computing:

Most businesses start using electronic infrastructure. Desktop machines are forced to migrate into the desktop due to significant cost savings and efficiencies. A well-designed infrastructure and operational security preparation would allow businesses to handle cloud computing threats effectively. However, recent studies and research show that the value of protection due diligence remains overlooked by companies when it comes to vetting these suppliers. When cloud usage grows in 2012, new cases of intrusion will demonstrate the complexities of forensic analysis and incident response by these providers, and the question of cloud protection will be given due consideration.

D. Protecting networks instead of details:

The focus will be on data protection, not just systems. When consumers and businesses are like going to store more and more of their important information online, the security requirements will go beyond merely maintaining systems to protect the data that house these systems. The protection of data stored in these systems would require greater granular control-from the users and organizations-instead of

concentrating on designing mechanisms to secure system information housing.

E. New Systems and facilities:

New platforms and apps can offer cyber criminals new opportunities. Yet new platforms and new devices, including iphones, iPods and Ios, would likely create additional menaces. Android phone's first Trojan watch this summer, and malicious apps and spyware appear to be reportable and not just on Ios. Anything concrete can be recorded. The personal notes on paper, binder, and even photographs on the wall can be replicated remotely and derived resources to make a breach of protection by the protester sort, and that is a concern more and more.

F. Practices and Concerns of Cybersecurity from Government Agencies:

Join the criteria of all residents and not just of democratic governments in domestic information security strategies. Promoting the broad acceptance and use of the Convention on Information-Crime and other future international agreements. Help encourages instruction as not only the individual client and program gains, but also eliminates the amount of exposed devices accessible for offenders to be hijacked for assaults.

II. CYBER CRIME

The definition of cybercrime extends by the US Department of Justice to include any illegal activity that uses a computer in order to save evidence. Cybercrime represents a term for any illicit activity that uses a computer as its main means of commissioning or theft. The ever-growing list of cybercrimes involves code-imposed offences, such as network intrusions and computer virus distributors, and web-based forms of traditional crimes like identity theft, harassment, intimidation and extremism that have become a major problem for individuals and nations. Typically, cybercrime can be described in common man's vocabulary as a crime committed using a computer and Internet to steal the identification or sell a person's pornography or to harass victims and interrupt operations involving malicious programs. As technology plays a major role in the lives of a person day by day, cyber crime will also continue as technological developments progress.

III. CYBER SECURITY

Health and data protection will always be the main healthme asures for all businesses. We are currently living in a world of digital or cyberformat knowledge. When you interact wit h friends or family, social network sites provide a safe envir onment for users. In the case of home users, cyber criminals will continue to target social media websites throughout order to steal personal data. In addition, a person must take all necessary security measures during banks and social networking.

Table 1: Comparison of number of incidents b/w Q1 2017 and Q2 2017

Categories of Incident cases	Quarters		Percentage (%)
	Q1 2017	Q2 2017	
Content Related	16	13	-18.75
Cyber Harassment	150	229	52.67
Dos	14	7	-50
Fraud	803	909	13.2
Intrusion	447	523	17
Intrusion Attempt	90	71	-21.11
Malicious Code	227	225	-0.88
Spam	88	93	5.68
Vulnerabilities Reports	15	8	-46.67
Total	1850	2078	12.32

Source:https://www.ijerm.com/download_data/IJERM0507021.pdf

Table 2: Number of incidents reported in the months of Q2 2017

Categories of Incident cases	April	May	June
Content Related	2	9	2
Cyber Harassment	71	119	39
Dos	3	1	3
Fraud	265	346	298
Intrusion	101	138	284
Intrusion Attempt	41	22	8
Malicious Code	62	92	71
Spam	30	31	32

Source:https://www.ijerm.com/download_data/IJERM0507021.pdf

MyCERT revealed the cyber security risks that were higher in compared with cyber security events that can be identified by MyCERT From April to June 2017, from Q1 2017 to Q2 2017. Perhaps the security precautions are rising with violence. The Silicon Valleys geographic area (geographic region) is aligned with the study of U.S. technology and care executives nationally. Financial institution noticed that companies consider hacking attacks constitute a significant security risk to their information and continuation of operation.

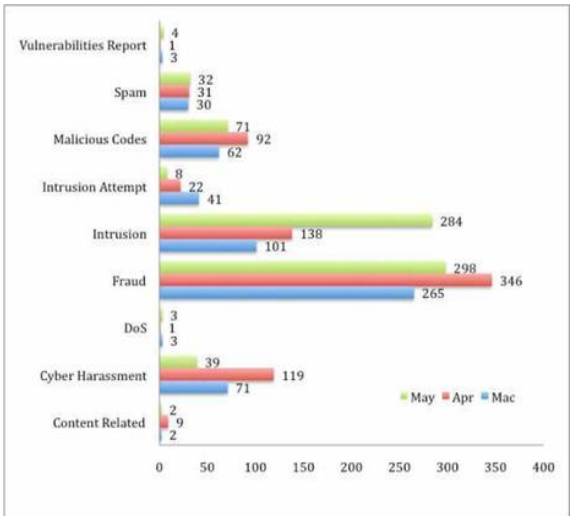


Figure 1: Breakdown of Reported Incidents in April to June 2017

Source:https://www.ijerm.com/download_data/IJERM0507021.pdf

Cyber security challenges are obvious from this review of cyber security reported incidents in India from April to June 2017. The high level of violence thus increases safety precautions. 98% of businesses keep or improve their protection, but several are growing this year's funding for electronic threats. Though the smart city trend also produced many interconnected communities, an unpreparedness for cybersecurity still poses significant weaknesses to protection. Only one-third was totally confident regarding the current protection of their company associates ' documents and therefore less confident about any safety precautions.

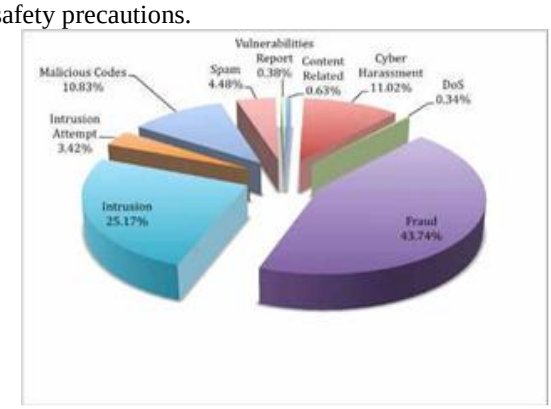


Figure 2: Percentage of reported incidents by classification

Source:https://www.ijerm.com/download_data/IJERM0507021.pdf

A. Patterns Changing CYBER SECURITY

Several of the developments who have a major effect on information protection are described below. Web servers: The probability of cloud apps affecting information resources or distributing malware programming continues. Cyber criminals spread their encrypted data through legal, hacked web servers. But data-stealing crimes are also a massive threat, many of which get media attention. Today, further focus is required on securing web servers and web applications. Web servers in particular provide these fraudsters with the perfect platform to hack the info. Thus, in addition not to suffer as a prey for these violations, one must always use a safer browser particularly throughout major trades.

B. Cloud computing and its services

Today, cloud services are increasingly being embraced by all small, smaller and larger businesses. That is, the world moves gradually to the clouds. This latest craze raises a major cybersecurity issue, since it can travel through conventional enforcement locations. However, as the number of developers accessible in the cloud increases, security mechanisms will have to be implemented for web applications and cloud services in order to insure that valuable information is not lost. Although the cloud services build their respective templates, their protection also poses several issues. Cloud will offer huge possibilities, but it must be remembered at all occasions that the cloud develops to raise its security problems. APT and the APT threats are a different level of cybercrime technologies (APT, Advanced Persistent Threat). Network security technologies like web filtering and IPS were an important factor for decades in the recognition of those goals (mainly until the preliminary compromise). When attackers are stronger and use more cryptic tactics, defense network needs to be incorporated into other spy agencies for attack detection. Therefore our protection procedures need to be strengthened in order to prevent any threats.

C. Mobile Networks

Currently in every part of the world we will link to anyone. Nevertheless, health is a very major issue for these wireless networks. Firewalls and other security measures are becoming vulnerable nowadays, as citizens use apps like laptops, telephones, PCs, etc, which, apart from the programs, require additional securities. The safety problems of such mobile networks must always be discussed. Many mobile networks are extremely vulnerable to each of these digital attacks and need to be very vigilant with their safety concerns. Ipv6: New protocol for internet Ipv6 is a new protocol replacing ipv4, a cornerstone to our systems in particular and the web as a whole. protection is not just about ipv4 porting. Although ipv6 is a mass substitution for having additional IP addresses, some very simple improvements to the protocol must be taken into consideration in security policy. Therefore, it is best to move to ipv6 as early as possible to minimize the cyber crime challenges.

D. Encryption of the code

Encryption is the encoding method of documents (or knowledge) in a manner that attackers or cybercriminals cannot interpret. The document or data is authenticated with an encryption method in a cryptographic framework and converted into an unusable cipher script. It tends to happen using an encryption key, which determines how to decrypt the letter. Encryption preserves the secrecy and confidentiality of information at an early stage. Nevertheless, expanded use of cryptography creates new safety problems. Cryptography can be used for transit data protection such as network communication, such as email, e-commerce, mobile phones, wireless microphones, cellular communications etc. Wireless intercoms. Therefore you can learn whether there is any security exposure by accessing the file.

Nothing new under the sun of the Attack Vectors chart, where Malware ranks on top with 41.1% (from 37%), ahead of Account Hijackings stable to 14.2% from 13.9%. Attacks driven by Vulnerabilities jump at number three among the know vectors with 11.3%.

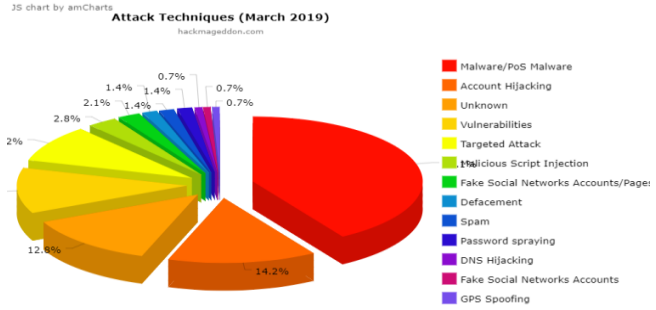


Figure 3:The top network threats are mentioned in below

Source:https://www.hackmageddon.com/2019/04/17/march-2019-cyber-attacks-statistics/

E. Role of Social Media In Cyber Security

Through globalized world we are rising socially; businesses need new ways of safeguarding personal data. Social media performs an important part in public protection and contributes significantly to immediate cyber threats The use of social media by staff is booming, and so is the threat of attack. Since most of us do using social media or social media platforms daily, it seems to be an immense forum for malicious hackers to search and seize personal information. Many businesses cannot legally stop accessing social media because it plays a key role in an industry's marketing, even if social networks can be used for cybercrimes. We should therefore provide ways to warn them of the hazard, so that it can be resolved before any damage is done. Organizations will, therefore, consider this and recognize the importance of review of details specifically in social debates and provide adequate safety strategies to prevent damages. It's about using certain techniques and correct resources to manage the social media.

IV. CYBER SECURITY TECHNIQUES

A. Access Control and Password Security

The **username** and password concept has become an essential means of protecting our data. This could be one of the first cyber security initiatives. Until uploading it is necessary to check whether the reports that we obtain come from a trustful and trustworthy source and whether they are not modified. Effective antivirus software is therefore essential in order to defend computers from viruses.

B. Malware scanners

The program normally checks for malicious code or dangerous viruses all the data and documents stored on the device. Viruses, worms and trojan horses are instances of malicious software, sometimes mixed and named malware.

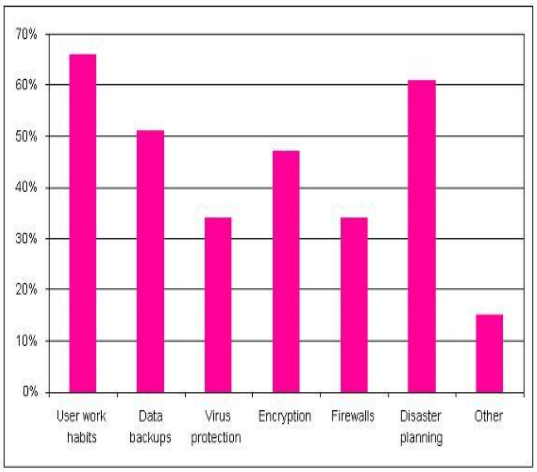
C. Firewalls

A firewall is a software or hardware program that helps to track malware, malware and worms who seek to enter the machine through the internet. The existing firewall scans all communications that enter or leave the Internet and prevents those that do not follow the defined safety requirements.

D. Anti-virus software

The antivirus program is a software program that identifies or avoids malware activities such as viruses and worms, and actively works to disable or kill them. Many antivirus applications provide an auto-update service that allows the system to download new virus types and ensure that they are being detected. For every system, antivirus software is a must and utter prerequisite.

Table 3: Techniques on cyber security



Source:https://www.ijerm.com/download_data/IJERM0507021.pdf

E. Cyber Ethics

Web ethics are only the internet language. If we exercise such web principles, we are likely to make better and safer use of the web. Some of them are below: Do not use the Web to connect with and talk with others. E-mails and text messaging promote contact with family and friends, correspondence with employers and the exchange of ideas and knowledge between others around the city. On the Net, don't be a tyrant. Do not call people, complain about them, give them embarrassing photos or do anything else to harm them. The Internet is considered the largest library in the world, with information on every subject of any kind, and it is therefore necessary to use this information correctly and legally. Do not use the credentials to access certain accounts. Never attempt to submit malware of some sort to render it malicious to any systems. Never disclose your confidential details to anybody because it can be misused by someone and you wind up in trouble. If you're online, never seek to make false profiles for another person, because that will enable you and the other user to get into trouble. Copyrighted content should always be protected and games or videos should be accessed only when allowed.

The below are a number of cyber ethics to use the web from very initial phases we have always claimed that the appropriate principles are equivalent nowadays in cyberspace. Expand the development of advanced informatics and policing. Help the worldwide Computer Emergency Response Team (CERT) by donations as the most possible way to prevent or alleviate a major Internet crisis. Fund research in fields such as: improved protocols on the Net, risk analysis, strategic planning and catastrophe dissemination study, human system consumption variables, defense economies.

Necessary counter-measuring methods, consumers and organizations, following good Internet security procedures, will improve resilience and sensitivity to defend themselves against several threats or to reduce the potential effects of accidents. Set up and change in operating systems modules as well as other computer programs accordingly. Firewalls, anti-virus and anti-spyware applications are used and updated regularly. It may become the object of identity or assets, based on the details you disclose.

V. CONCLUSION

Cyber securities are an important problem and there is a strong connection between the internet and systems to perform sensitive activities. There are major risks for several companies, institutes, government sector (exceptionally important development). The Cyber Security strategy throughout all its dimensions will be critical for development, creativity and advantage for corporations alike. There really is no single solution to sustainability, but companies will move towards a potential world that is transparent and stable and prosperous by collaborating through the government and industry alliances by supporting safety measures, in general in relation to task-critical systems, procedures and technologies that are related to cyberspace.

Since cybersecurity is not just a technological task, a successful global cybersecurity team would require a wide variety of experiences and expertise. The big issue seems as though development is evolving every day, and so are creative ways of exploiting cyber security for the malware and the cyber terrorism tactics. Regarding the interconnected complexity of developing economies and hence the integration between different communication systems, it is important that there is common culture around the world toward that cybersecurity risks. In order to manipulate security problems, the financial services industry will proceed through strong defensive potential.

VI. RESULT AND DISCUSSION

Computer protection may be a massive problem, because the world is increasingly interactive, with databases being accustomed to carrying out valuable activities. For the Millennium Year that goes, cyber-crime begins to evolve from new approaches, and then data security. Along with the latest security techniques and risks that rise to light weight on a regular basis, the latest and turbulent systems make challenging organizations to not just protect their assets, but also require different resources and knowledge and seek and do so. Though, there seems to be no successful remedy for cybercrimes.

Nevertheless, proportional response is not adequate. Due to the ongoing and changing existence of cyber security challenges, a universal accountability, obligation and deterrent arrangement must be formed at the increasingly violent border of cyber warfare.

REFERENCES

1. . Computer Security Practices in Non Profit Organisations – A NetAction Report by Audrie Krause. (NetAction is a project of The Tides Center601 Van Ness Ave., No. 631 * San Francisco, CA 94102 Phone: (415) 775-8674 * Fax: (415) 673-3813 * E-mail: info@netaction.orgWeb: http://www.netaction.org)
2. G.Nikhita Reddy, G.J.Ugander Reddy (2013), " Study of Cloud Computing in healthcare Industry", International Journal of Scientific & Engineering Research, Volume 4, Issue 9, September-2013 Page nos.68 – 71 ISSN 2229-5518.
3. IEEE Security and Privacy Magazine – IEEECS "Safety Critical Systems – Next Generation "July/ Aug 2013.
4. 4. Nina Godbole and Sunit Belapure (2011), "Cyber Security: Understanding Cyber Crimes, Computer Forensics And Legal Perspectives", New Delhi, Wiley India Pvt Ltd. SBN-13: 978-8126521791 ISBN-10: 9788126521791
5. Luis corrons – Panda Labs (2013) A Look back on Cyber Security 2012, CIO Asia, September 3rd, H1 2013: Cyber security in Malesia by Avanthi Kumar.)
6. Kellermann, (2014) "Technology Risk Checklist, Cybercrime and Security", IIB-2
7. Peter Sommer, Ian Brown, (2011), OECO Project, "Reducing Systemic Cyber Security Risk", IIB2.
8. Booz Allen and Hamilton, Reports, (2012), "Top Ten Cyber Security Trends for Financial Services" Business wires, Berkshire, Hathaway. ,
9. A Sophos Article 04.12v1.dNA, eight trends changing network security by James Lyne.
10. CIO Asia, September 3rd, H1 2013: Cyber security in malasia by Avanthi Kumar.
11. www.hackmageddon.com/2019/04/17/march-2019-cyber-attacks-statistics/
12. Kellermann, "Technology Risk Checklist, Cybercrime and Security", IIB-2
13. Peter Sommer, Ian Brown, OECO Project, "Reducing Systemic Cyber Security Risk", 2011
14. Booz Allen and Hamilton, Reports, "Top Ten Cyber Security Trends for Financial Services", 2012

AUTHORS PROFILE

Dr. Hena Iqbal have doctorate degree (Ph.D.) from India and have been teaching for the past many years in UAE. She has been also teaching in India for more than 4 yeaars (IGNOU, MANIPAL, C.M. College). As a teacher, her main goal is to motivate students to do their best and extend their own personal limits. She devises programs, according to the syllabus requirements, that expand on previous knowledge and encourage students to explore new and interesting possibilities. She had experienced many opportunities to work with a variety of professional learning teams and have gained valuable insight into the role of Lecturer in University. On each occasion she had worked and managed to demonstrate excellent planning, communication and team work skills. She is very active in her research work also. At present she is working as an Assistant Professor in IT department at Al Dar University College, Dubai, UAE.

Professor Ghassan Al-Utaibi, PhD is highly experienced and successful academic, and business consultant with extensive experience and a proven track record of successful consulting projects in the UAE, Jordan, and the UK, among other countries. He specializes in decision support and scenario planning for future foresight and strategic planning. The areas of expertise include working with major international organizations such as the United Nations Development Program in a number of countries, the USAID, USTD, the German Agency for Technical Cooperation, and the Arab Administrative Development Organization. Projects implemented in the UAE focused on education, excellence, strategic foresight. Prof. Al-Utaibi designed an award for excellence with a major component related to innovation management. He has over 20 years of experience in excellence awards assessment especially in the UAE and also in providing advice related to the qualifying of institutions for these awards. Profile which contains their education details, their publications, research work, membership, achievements, with photo that will be maximum 200-400 words.

Dr O P Bohra has obtained his education (Graduation and Master from Jodhpur University and Doctorate from University of Rajasthan) India. Since last 12 years he was teaching at various business schools/universities in India and different universities in Dubai, Abu Dhabi, Sharjah (UAE.) In the research field he was associated as an Economist with National Institute of Public Finance and Policy, New Delhi, India for a long span of time. For the collaborative research work he had worked with University of Cambridge UK. He had undertaken many consultancy assignments with World Bank. His research interest includes, largely, in the areas of Management, Finance, Public Finance and Fiscal Decentralization and Corporate Social Responsibility. In India, he is also holding a honorary position of member of Board at SriSIIM, India and was holding an honorary position of Chairman Senate, and Professor of Eminence at SriSIIM, New Delhi. Presently, Dr Bohra is Chair, Business Administration, School of Business Administration, Aldar University College, Dubai (UAE)