ANALYSIS ON CHALLENGES AND THREATS IN CYBER SECURITY

Dr.A.P. Nirmala, Sravana N

Abstract- Cyber security is a information technology. Securing information has become one of the biggest challenges nowadays. Whenever we think about cyber security the first thing we remember is 'Cyber Crime' which is been increasing day by day. The cyber security is still a very big concern to many. This paper mainly focuses on challenges faced by cyber security and its types. To the world of computer technology, governments, police and intelligence units are acting toward the issue closely. Different strategies are put into action. The main goal is to educate the people in the world and to expose the idea that it is not safe anymore to navigate in the cyber world without any of security. This paper discuss about techniques used in cyber security.

Index Terms- Cyber-security, computer security, Malware, Phishing, Viruses.

I. INTRODUCTION

Cyber security is a techniques developed to safeguard information stored on computers. It is designed to protect network, programs and data from attack, damage or unauthorized access. The attacks are usually aimed at accessing, changing or destroying sensitive information, extorting money from users. Today in the world the man is able send and receives any of kind of information through email, audio or video just by clicking the button itself. But he never thought how securely his data id is been transmitted to other person safely without any flow of information? .Now days internet is the fastest growing foundation in day life. We are not able to protect the private information in a effective way and hence the cyber crime is increasing day by day. The 60% of commercial transaction are done through online; this field required a high quality of security for the transaction. The cyber security is not limited to secure the information in IT industry it is also to other fields like cyber space. Increasing the cyber security and securing the information are essential to each nation security .The fight against the cyber crime need a safer approach. Many nation and government are having strict laws on cyber security to prevent the loss of some information. Everyone must also be trained on this cyber security and save them from the cyber crimes.

Cyber security is been widely recognized as essential by individuals, firms and governments [1]. As the society has grown more dependent on information system and the Internet, the need for secure and reliable. As the requirement has been spread beyond the domains of computing and information technology, the number of disciplines contributing valuable perspectives has also expanded greatly. For instance lawyers, social scientists, and policy scholars help to improve our understanding of how people and institution make decision affecting security and privacy. The computer scientists, engineers and cryptographers have begun designing secure technologies that take personal or institutional incentive into account.

Privacy and security of the information will be in top security measurement that any organization takes care. Cyber security is important because the military, corporate, government, financial and the medical institute will collect and store amount of data in computer. The organization will be transmitting the sensitive data throughout the network and other device in course of running businesses.

II. CHALLENGES AND THREATS IN CYBER SECURITY

Cyber Security refers to ensure the data stored in a computer cannot be read by any individuals without authorization. Cyber Security involves data encryption and passwords.

The threats involved in cyber security across the three datasets. Figure 1 illustrates their prominence in the entire corpus. In all of the security education materials

we gathered, the most commonly discussed is *Phishing and Spam.* The second most common topics, with roughly the same prevalence in the entire corpus, are *Data Breaches* and *Viruses and Malware*. The least is *Mobile Privacy and Security*. Stories, with a mean word count of 95, were much shorter than both news articles ($M = 617$) and web pages ($M = 971$). Both the news article and web page datasets had a number of outliers that were significantly longer than other documents. In the news dataset, 12 items (1%) were longer than 2000 words ($M = 3152$, $SD = 1709$). Thirty-one items (6%) in the web pages dataset were longer than 2000 words ($M = 3763$, $SD = 1972$). Table 1 has additional descriptive.

Type	Mean	Median	SD
Web pages	**795**	**566**	**972**
News articles	**617**	**532**	**458**
Personal stories	**95**	**83**	**50**

Table 1 Calculation of Mean, Median and standard deviation.

LDA assumes that each document in a corpus is composed of *all* topics. However, some topics are more prevalent in any particular document than others. This allows us to identify which are most commonly discussed. The weight of each topic in the full corpus is listed in Table 2. Nearly all documents consist of at least two or three topics with a weight greater than 0.10. For each topic, we counted the number of documents that had that topic listed as the primary topic (largest weight for that document) and the number of documents that listed the topic as the secondary topic. On average, the primary topic had a weight of 0.56 ($SD = 0.17$), and the secondary topic had a weight of 0.21 ($SD = 0.09$).

Topic name	Corpus Weight	Main		Second	
		#	%	#	%
PhaS	0.27	266	14	286	15
DtBr	0.23	220	11	241	12
VraM	0.23	243	13	220	11
HaBH	0.23	139	7	282	15
PsaE	0.20	139	7	170	9
NtnC	0.19	245	13	181	9
CCaIT	0.19	166	8	177	9
PaOS	0.17	124	6	143	7
CrmH	0.14	239	12	107	5
MPaS	0.10	101	5	75	4

Table 2.Percent Document.

"Corpus weight" is the weight of each topic by the LDA (latent Dirichlet allocation) algorithm across the entire corpus. "Main topic" and "Second topic" show the number and percent of documents in the entire corpus with each topic as the most prevalent topic in the document, and as the second most prevalent topic in the document.

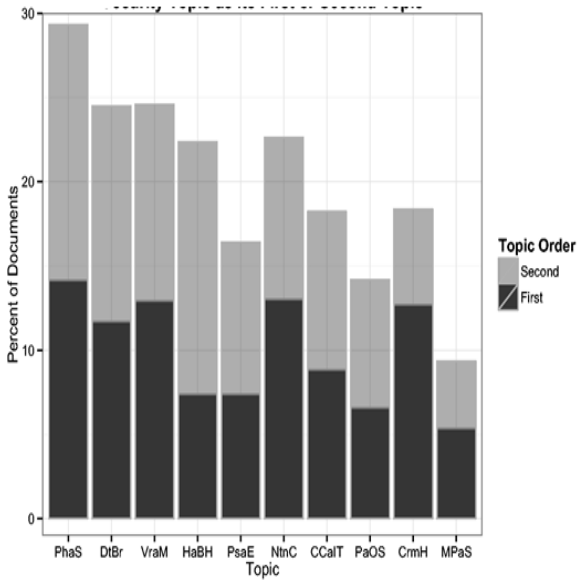

Figure 1.Percent of Documents Having Each Security as its First or Second

A. Phishing and Spam (PhaS)

"email information account phishing mail message spam personal Internet site website address messages click password web facebook links link"

Phishing is a common form of online scam where criminals attempt to trick users into revealing sensitive personal information via emails that upon first glance can appear genuine, but in reality are not [7]. The information users reveal is then typically used for financial or Internet fraud. Phishing and Spam are a large problem with email in society right now. Approximately 1 in 900 emails was a phishing scam in 2014 [8]. Every day, about 28 billion spam emails are sent around the globe. Dhamija *et al*. [9][10] Found that these types of attacks work because most users are either not aware of indicators of scams or do not pay attention to such indicators. Since these types of scams directly target and exploit end users, end users need education to protect themselves from such attacks. Out of the 10 topics we identified, *Phishing and Spam* was the most prevalent in the corpus, with overall weight of 0.27. Most of our documents about phishing focus on its delivery method, including words such as "email, account, mail, spam." Many documents that have high weights for this topic include definitions and examples of phishing (including specific forms like "spear phishing" and SMiShing), advice for how to identify phishing both before and after one has become a victim, what to do if you become a victim, and tools to help users avoid being exposed to phishing scams. Some documents try to help users identify what phishing attacks look like, and give examples of tactics scammers use to prevent the messages they create from being blocked by spam filters. Many include reminders that companies like banks and employers will not send requests via email asking for login credentials or other personal or account information. Finally, a few documents describe tools such as browser plug-in and spam filters that help users to not become victims.

B. Data Breaches (DtBr)

"data sony customers information hackers breach online network attack users services accounts playstation attacks personal service systems customer card"

This topic focuses on instances where user information (account details or other personal data) were exposed by "hackers" or "attacks," or by users inadvertently revealing information publicly that should have been kept secure. Data breaches are a growing problem. In 2014, 312 companies publicly reported a breach that exposed data from approximately 350 million users, such as real names, government ID numbers (e.g., US Social Security Numbers (SSN)), home addresses, and financial information [8]. Fifty-seven percent of Europeans reported having their information exposed at some point in the past via a data protection failure or data breach [11]. Data breaches also affect corporations; firms notice a drop in their stock prices after announcing a data breach that involves confidential information [12].How a breach occurred is usually unknown or goes unreported; instead, the documents focus on the aftermath in terms of costs to both organizations and users. A number of other attacks were included as part of this topic as well. For example, distributed denial-of-service attacks and other security-related events that caused systems to become unavailable used words like "online, services, systems," which are part of this topic. In addition, there were several real-world examples in which files containing personal data (SSNs, health records, drug, and alcohol test results) were exposed publicly on the Internet by mistake when they should not have been, causing embarrassment and potential liability for the organizations at fault.

C. Viruses and Malware (VraM)

"computer software antivirus malware windows internet Microsoft spyware program viruses firewall malicious programs file files computers system install"

This topic focuses on educating users about "viruses." It contains definitions of viruses, malware, spyware, adware, and worms that are aimed at informing users about the nature of threats from malicious software that self-propagates or spreads after the user has taken some action. These definitions sometimes included detailed descriptions of particular malware (e.g., DNSChanger, Koobface, Mac Defender), or a history of the evolution of computer viruses. Symantec reports that 317 million new pieces of malware were created in 2014 . This represents almost 1 million new pieces of malware every day. Approximately 1 in 244 emails included a malware attachment or a link to malware [8]. End users frequently think about viruses, and use the term "virus" to represent all malicious software . There are many different kinds of malware, and users have difficulty understanding the threats and taking action to protect their computers [13]. Instead, they often

delegate that responsibility to software tools like antivirus [14].

Much of the content in this topic is focused on how to avoid being compromised or infected. Tools like antivirus are mentioned frequently, as well as antispyware and firewalls. However, there is also a lot of behavioral advice, such as admonitions not to use p2p file sharing software, and to download only trusted software. This topic also includes advice to install software updates regularly. Finally, this topic includes descriptions of the kinds of symptoms users experience when using a computer that may have been infected. These symptoms are often nonspecific, like slow performance, pop-up windows in a web browser, or settings that have been changed—things that are very difficult for users to attribute directly to malware. This topic contains very little about what users should do to cope if they experience symptoms like this, or who to turn to for help.

D. Hackers and Being Hacked (HaBH)

"Hacker computer money asked wrote hacked wanted hard eventually hacking game worked left twitter idea night gave half reason"

There are a variety of different contexts and interpretations in which the word "hacker" is used. It usually means someone who is technically skilled that breaks into computers to gain unauthorized access, but it can also mean an especially talented or skilled programmer. Because "hacker" is an overloaded term, the mentions of hackers in the corpus range widely and also do not overlap very much with each other. For example, documents that depict pop culture impressions of hackers include discussions about the movie "Girl with the Dragon Tattoo," which was released in 2011 in the USA and featured a hacker (someone who breaks into computers) as one of the main characters. There were also documents reviewing books that had been published about famous or well-known hackers, or written by hackers about hacking.

This topic also includes descriptions of things "good" hackers do, like attend hacker conferences and work for the government or companies to try to identify vulnerabilities. It also includes the idea of "hacking" as demonstrating one's skill as a programmer, and using those skills to generate new ideas and invent new things. There were also mentions of the Silicon Valley "hacker ethos" as a way of solving problems. Finally, this topic includes depictions of hacking as criminal activity, although there are few specifics about exactly how that activity is undertaken. Instead, the documents included examples of compromised computers or systems. The Sony Play station hack appears in this topic as well, but depicted as a "hack" rather than a data breach. There were many mentions of high-profile celebrity account compromises, also referred to as "hacks." There were also examples of problems with one's computer, like porn popup or other symptoms similar to those in the Viruses and Malware topic, but in this topic the source of the problem was attributed to an attack by a "hacker"—a person—rather than malicious software.

E. Passwords and Encryption (PsaE)

"Information data password network access passwords secure wireless computer system encryption public networks devices sensitive personal computers protect [wi]fi"

Many users are concerned about protecting their computers and safeguarding their digital information. This topic includes two main ways to do this: use encryption, and have good password habits and practices. In general, there is a tradeoff between security and usability. Highly secure systems such as email encryption are often difficult for people to use [15]. However, people do perceive that using stronger passwords makes them more secure [16]. This topic does not address the tradeoff; instead, it focuses on the behaviors and practices users can adopt to take full advantage of the benefits of these technologies. It also includes some information about physical security, such as watching out for shoulder surfing, and controlling physical access to one's devices, especially while traveling.

It advice about creating passwords, though always from a security standpoint rather than a usability standpoint. This includes descriptions of what a strong password looks like, some of which is contradictory: long, mixed case with numbers and symbols, avoid dictionary words, changed frequently—and yet easy to remember. It also addresses encryption in the context of wireless network security, including advice not to use open wireless networks, to check websites to make sure they use SSL, and how to configure a home wireless network to make it more secure.

F. National Cyber security (NtnC)

"Government cyber internet attacks computer china official's state military Iran attack systems united national states department nuclear Chinese networks"

Documents in this topic cover computer security in relation to national security concerns. In recent years, cyber attacks either against or allegedly perpetrated by governments have gained widespread coverage and attention, and have also been increasing in frequency. There is much concern about the future of cyber warfare, and the role the security of global networks and infrastructure such as water supplies and the electric grid may play [17].

In our corpus, this topic included specific examples of cyber attacks such as Stuxnet; instances of online espionage; attacks against the US State Department, White House, and Chamber of Commerce; and discussions of whether or not such attacks should be classified as acts of war. There was also coverage of what should be done to protect critical infrastructure from attack, and the marshaling of national security resources such as recruiting "white hat" hackers, and training for the military in cyber warfare. In addition, this topic included discussions of repressive regimes and authoritarian governments using tactics to restrict access to the Internet. There were stories about when Egypt shut down access to the Internet in January 2011, mentions of Internet censorship by Iran and China, and Russia jamming Smartphone as a protest in 2011.

G. Credit Card and Identity Theft (CCaIT)

"credit information identity theft card report bank number fraud personal account money social online accounts consumer file contact victim"

Identity theft and financial fraud are topics of considerable concern. Identity theft is a growing problem, and is associated with computer security because often the information necessary to steal someone's identity is obtained through compromising enterprise or business systems, or through email or other online scams that trick people into compromising their accounts. A stolen credit card can be sold in the black market for anywhere between $0.50 and $20.00; a scan of a real passport is worth about $1–$2; and a stolen gaming account can be sold for as high as $15 [8].

It contains definitions of identity theft, primarily related to criminal efforts to commit financial fraud by obtaining or using credit in someone else's name. It includes definitions of what identity theft is, depictions of the emotional cost and stress of dealing with identity theft, and how to cope with the consequences and aftermath of becoming a victim to identity theft. In addition, this topic includes more detailed and specific advice and instructions for how to prevent identity theft. For example, many documents describe what kind of information a criminal would need to steal someone's identity, and how they might obtain that information. Some documents recommend using strong passwords for financial accounts as a way to prevent criminals from accessing them, and even using cash instead of credit cards to pay for things. Finally, this topic covers how to recognize signs that one has become a victim of identity theft, including strategies such as regularly monitoring accounts and obtaining one's free yearly credit report.

H. Privacy and Online Safety (PaOS)

"Online facebook social information privacy internet sites kids users children personal web child networking share post content safety protect"

It contains information about staying safe online. Much has been written about interpersonal risks associated with Internet use. These risks include unwanted disclosures, interactions with bullies and others out to do harm, and hostile online situations that can transition to real-world dangers. Many people believe that privacy and online safety are personal issues and that we should place personal responsibility on end users for their online safety [18][19].

Present in documents associated with this topic are discussions of privacy issues related to the use of online social networks, and effectively managing one's digital footprint. In particular, many documents focus specifically on Facebook and using location-based services as activities that involve particularly strong risks. Online bullies, harassment, and sexual predators are among the negative safety outcomes associated with Internet use that we found in the corpus. For example, there are descriptions of the behavior of online predators, and advice for parents on how to identify when children might be involved with one. Cyber bullying also appeared in the documents as part of this topic, as well as exhortations not to become someone who bullies or intimidates others online. Finally, many documents contained online safety tips for parents and children to help them stay safe online. These tips included age-based guidelines for appropriate Internet use, information for parents about age-appropriate limits, and other advice not to trust everything people say online or meet up alone with someone from an online forum or chat room.

I. Criminal Hacking (CrmH)

"Police anonymous computer hacking lulzsec wikileaks law court crime twitter hackers manning website arrested hacker cyber posted investigation members"

This is made up of examples and instances of cyber crime. It is distinct from "Hackers and Being Hacked" in that it is entirely focused on the criminal acts that may be perpetrated by "hackers," and any legal consequences that may occur. Cybercrime can include traditional crimes that are now conducted online (such as harassment or stalking), crimes that have substantially changed as they have moved online (such as credit card fraud), and new crimes that are solely online (such as creating botnets). While most of the costs of cybercrime to victims are based in traditional crimes moving online, most security expenditures go toward the new crimes [20].

It contains general descriptions of criminal activity involving digital technologies, as well as reports of the prevalence of said activity. For example, some of the documents in this topic contain descriptions of the crimes and consequences in the legal system of activities like harassing, stalking, and spying on others using computers. This includes things like hacking webcams to access naked pictures and video streams of women, spouses spying on each other, etc. In addition, this topic includes instances where the criminal activity resulted in some public display or evidence that a hack had taken place, like taking over and defacing an organizations website or posting offensive things on its social media account, and posting information like passwords or confidential documents that were obtained through the criminal activity on some public forum or other website. Finally, this topic includes documents talking about Anonymous, WikiLeaks, and Lulz Security that some might classify as "hacktivism." The activities of these entities are treated in most of the documents that mention them as instances of cybercrime.

J. Mobile Privacy and Security (MPaS)

"Mobile phone apps device Google app devices apple data android users cloud phones location Smartphone store market malware software"

This topic contains information about privacy and security related to mobile devices. This is its own topic, rather than falling under other topics related to privacy and security, because the discussion of mobile security is different from other kinds of computer security advice. Because mobiles are easier to lose and therefore fall into others' hands more often, physical device security is a concern addressed in this topic. Also, approximately 17% of apps on the Android apps store were malware in 2014 [8]; therefore, the app download and software update model are aspects of mobile privacy and security that do not exist in the same way for other kinds of computing devices. As a result, users tend not to think of their mobiles in the same way they do their personal computers, for security and privacy purposes. Few people use antivirus for their mobiles, and few understand that Smartphone and tables can be vulnerable in the same ways computers are. These beliefs were reflected in this topic.

Many of the documents focused on trying to educate and encourage users to adopt better mobile security practices, by communicating things like how mobile apps can be shady from a security and privacy perspective, and that users should be very careful when downloading and installing apps. Mobile app permissions and the risk of spyware and tracking technologies in particular, were discussed. Finally, the documents made a platform-related distinction between Apple and Google, and the review policies of the different app stores for mobile apps. In particular, Apple makes more of an effort to review submissions to its app store than Google does. This ostensibly means more malware is available for Android, and Android users must therefore be more careful than iOS users. This was illustrated in our corpus by more documents about security tips for the Android platform than the iOS platform.

III. ROLE OF SOCIAL MEDIA IN CYBER SECURITY

Social media will play a huge role in cyber security and it will contribute a more to personal cyber threats. Information security is important these days to anyone who are using computer or to any organization that employ computer in their day to day operation. Information security should be as most important in mind since it is our personal information is there on the Internet. It states the information security is necessary because the information will be disclosed or used in the wrong way or to wrong person. Information security is divided into 3 major parts, which are called as CIA of information security. The parts are confidentiality, integrity, and availability. In Confidentiality only authorized people can access the information. In Integrity the

information is not tampered or corrupted in anyway. In Availability the information can be accessed and it is supposed to be. Since we became more social in increasingly connected world, the companies should be finding new way to secure their personal information. Since social network are used by most of them in daily life it has become a huge platform for the criminals for hacking the private information or data. However, mainly the companies should recognize, how much important of analyzing the information especially in social conversation.

IV. CYBER SECURITY TECHNIQUES

A. Access control and password security
The username and password is been fundamental way of securing our information. It may be one of the measures regarding cyber security.

B. Authentication of data
The documents we receive must always be authenticated before it is been downloading and it should be checked if it has originated from a trusted and a reliable source and that they are not altered. This document is usually done by the antivirus software present in device. Thus good antivirus software is to protect the devices from viruses.

C. Malware scanners
The software that usually been scanned all the files and documents present in the system for harmful viruses. The Viruses, worms, and Trojan horses are examples of malicious software that are often referred to as malware.

D. Firewalls
The firewall helps to find out the hackers, viruses, and worms that try to reach your computer over the Internet.

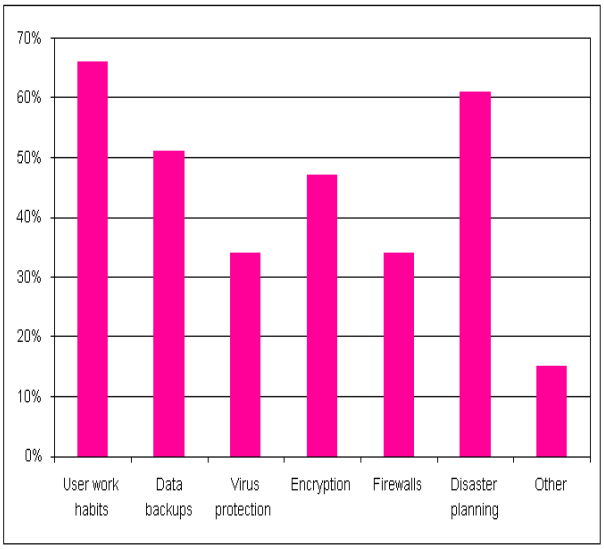

Fig .Techniques on cyber security

V. CONCLUSIONS

Cyber security is about managing future risk and responding the current and past attacks. The report has offered a highly standardized and clear model for processing risk-management information about critical information infrastructures. The cyber security is important because the world is becoming interconnected with networks used to carry out the transaction.

VI. References

1. Tyler Moore, David Pym .Oxford Academic ,Journal of cyber security ,volume 1, Issue 1, 1 September 2015, Pages 1–2,https://doi.org/10.1093/cybsec/tyv010,published 28 November 2015
2. Lawrence A. Gordon Martin P. Loeb William Lucyshyn Lei Zhou Journal of cyber security, volume 1, Issue 1, 1 September 2015, page 3- 17 ,https://doi.org/10.1093/cybsec/tyv011 Published**:**27 November 2015
3. Emilee Rader Rick Wash Journal of Cyber security Volume 1, Issue 1, 1 September 2015, Pages 121–144,https://doi.org/10.1093/cybsec/tyv008 Published:01 December 2015

4. GMO Global sign,Inc-[US]www.globalsign.com/en/blog/cyber security-trends-and-challenges-2018
5. IEEE Security and Privacy Magazine – IEEECS "Safety Critical Systems – Next Generation "July/ Aug 2013.
6. Hekkala, R., Väyrynen, K., & Wiander, T. (2012, June). Information Security Challenges of Social Media for Companies. In ECIS (p. 56).
7. Blythe M Petrie H Clark JA. F for fake: four studies on how we fall for phish . In:*Proceedings of the Conference on Human Factors in Computing (CHI) '11* , New York, NY : ACM , 2011 , 3469 – 78.
8. Symantec Corporation. Internet security threat report. 2015 .http://www.symantec.com/security_response/publications/threatreport.jsp (9 November 2015, last accessed date)
9. Dhamija R Tygar JD Hearst M/Why phishing work. In: *CHI '06: Proceedings of the SIGCHI Conference on Human Factors in Computing System*. New York : ACM , 2006 ,581 – 90.
10. Schechter SE Dhamija R Ozment A et al. . The emperor's new security indicators . In:*SP '07: Proceedings of the 2007 IEEE Symposium on Security and Privacy* . New York, NY: IEEE Computer Society , 2007 , 51 – 65 .
11. Symantec Corporation . State of privacy report. 2015 .http://www.symantec.com/content/en/us/about/presskits/b-state-of-privacy-report-2015.pdf (9 November 2015, date last accessed) .
12. Campbell K Gordon LA Loeb MP et al. . The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *J Comput Secur*2003 ; 11 : 431 –48 .
13. Wash R. Folk models of home computer security. In:*Symposium on Usable Privacy and Security (SOUPS)*. New York, NY: ACM , 2010 .
14. Dourish P Grinter RE De La Flor JD et al. . Security in the wild: user strategies for managing security as an everyday, practical problem . *Pers Ubiquit Comput* 2004;8:391 – 401 .
15. Campbell K Gordon LA Loeb MP et al. . The economic cost of publicly announced information security breaches: empirical evidence from the stock market . *J Comput Secur*2003 ; 11 : 431 48 .
16. Whitten A Tygar JD. Why Johnny can't encrypt: a usability evaluation of pgp 5.0.In *Proceedings of the USENIX Security Symposium* . Berkeley, CA : USENIX Association ,1999 .
17. Langner R. Stuxnet: dissecting a cyberwarfare weapon.*Secur Priv IEEE* 2011 ; 9 : 49–51 .
18. LaRose R Rifon NJ Enbody R . Promoting personal responsibility for internet safety .*Commun ACM*2008; 51: 71–76 .
19. Shillair R Cotton SR Tsai H-YS et al..Online safety begins with you and me: Convincing Internet users to protect themselves. *Comput Hum Behav* 2015 ; 48 : 199– 207.
20. Anderson R Barton C Böhme R et al. . Measuring the cost of cybercrime . In: *The Economics of Information Security and Privacy* . Berlin, Heidelberg: Springer , 2013 ,265– 300.

Dr. A. P. Nirmala, is presently working as Senior Assistant Professor in the Department of Master of Computer Applications, New Horizon College of Engineering, Bangalore, India. She has 16+ years of teaching experience. She has Published 10 Research papers in various National & International Journals including Scopus indexed. She also presented 12 research papers in National and International Conferences. She has published 2 Books on Operating system and Human Computer Interaction. Her research interests are Cloud Computing, Virtualization and Cyber Security. She is life member of CSI and ISTE.

Sravana N, student of New Horizon College Of Engineering in Department of MCA.