SENTIMENTAL ANALYTICS ON CYBER SECURITY AWARENESS FOR CITIZENS OF FINANCIAL INSTITUTES

Prof. Pushpendu P. Rakshit, Ph.D.
Research Scholar, Singhania University,
ITM Business School, Navi Mumbai.Maharashtra, India.
PhD guide- Dr. Anurag Shrivastava
Dr. Dy. Patil Institute of Management and Research.

Abstract: ***Since years, scholars like Kimball (2007),Lynne Yarbro (2008), Grace V (2009), Johnny Nhan(2010),Gable, Kelly(2010), Kyung-Shick Choi (2010), Smith, Katherine T.; Smith, L. Murphy; Smith, Jacob L(2011),Cindy J. Smith;Sheldon X. Zhang (2011), Paternoster (2011),Bradford W. Reyns (2012), E. Gabriella (2012), Jean, , Brody, Richard G.; Mulig, Elizabeth; , Redins (2012), Ngo, Fawn T, McMahon, Richard; Bressler, Martin S.; Bressler (2016),Williams,*** *Aditi Phadnis /***Business Standard** *reports National Crime Records Bureau, Analysis: IndiaSpend (2016),* ***Vivina Vishwanathan (2017) have addressed the concepts of cyber ethics, crimes and security aspects with the advancement in the trends of technology and move from traditional to online approach. Computer forensics as involving "the preservation, identification, extraction, documentation and interpretation of computer data (Kruse and Heiser, 2002) in the book Computer Forensics created an awareness that it is much of art than a science. Through the literature review from multiple dimensions, it gives a clear picture that computer / cyber security or related concerns are historic in nature. It is also used to include traditional crimes in which computers or networks are used to enable the illegal activity. The doctoral study is conducted on the customers using various modes of financial transactions across globe with their twit patterns on twitter to find the level of awareness regarding Computer forensics and literacy aspects along with further developments in the unexplored field of techno legal skill development, as it is one of the developed financial and commercial cities in modern era.***

The number of individuals victimized by computer crimes has increased annually (Gordon, Loef, Lucyshyn, & Richardson, 2004). Flana gan and McMenamin (1992) state computer Crime-committed by new generation of hackers might cost cybercrime victims,as a collecti ve, anywhere from$500million to $5 billion a year. TheComputer Emergency Response Team Coordination Center(CERT/CC) reports th at "the number of reported incidences of security breaches in the first three quarters of 2000 has risen by 54% over the total number of reported incidences in 1999" (McConnell International LLC, 2000, p.1).

Respondents were selected on the basis of twitter responses of almost 5000 respondents across globe to understand and study the crime trends and its impact, also to explore the relationship between increasing rates of cyber crime due to digitization and demonetization and customer awareness.

Key words: Cyber crime, Cyber forensic awareness, financial crimes, cyber attacks, cyber investigation cell, Indian government acts & laws, sentimental analytics forensic techniques, twitter, R tool .

Introduction:

Cyber crime is an umbrella term used to describe two distinct, but closely related criminal activities: cyber-dependent and cyber-enabled crimes.

Cyber-dependent crimes are offenses that can only be committed by using a computer, computer networks, or other form of ICT. These acts include the spread of viruses and other malicious software, hacking, and distributed denial of service (DDoS) attacks, i.e. the flooding of internet servers to take down network infrastructure or websites. Cyber-dependent crimes are primarily acts directed against computers or network resources, although there may be secondary outcomes from the attacks, such as fraud.

Cyber-enabled crimes are traditional crimes that are increased in their scale or reach by the use of computers, computer networks or another ICT. Unlike cyber dependent crimes, they can still be committed without the use of ICT. For the purposes of this review the following types of cyber-enabled crimes are included: fraud (including mass-marketing frauds, 'phishing' e-mails and other scams; online banking and e-commerce frauds); o theft (including theft of personal information and identification-related data); and o sexual offending against children (including grooming, and the possession, creation and/or distribution of sexual imagery).

The human social club has undergone terrific alteration from time to time with speedy pace at social level from the occurrence and technological level ever since the ascension of technologies. This technology world changes the human life in every manner and every sector. Banking field is one of them. Banking in India originated in the last decades of the 18th century. Since that instance the banking sector applying various ways to cater facilities and securities to a common man regarding to money. Security issues play exceedingly important portrayal in the implementation of technologies specially in banking sector. Further on it becomes more critical, when it comes to the cyber security which is at the nucleus of banking sector. After the arrival of Internet and WWW (world wide web) the banking sector has totally transformed specially in terms of security because now money is in your hand on a single click. Now user has number of choices to manage his money with different kind of methods. In my study an attempt has been made to put forward various issues of Indian banking websites / services for cyber-crime safety mechanism.

In 1979, Cohen and Felson proposed their routine activities theory, which focuses mainly on opportunities for criminal events. Cohen and Felson posited that there are three major tenets that primarily affect criminal victimization. The main tenets are (a) motivated offenders, (b) suitable targets, and (c) the absence of capable guardians against a violation (Cohen & Felson, 1979; Cohen, Felson, & Land, 1980; Felson, 1986, 1988; Kennedy & Forde, 1990; Massey, Krohn, & Bonati, 1989; Miethe, Stafford, & Long, 1987; Roneck & Maier, 1991; Sherman,

Gartin, & Buerger, 1989). The researchers argued that crime is likely to occur via the convergence of the three tenets. In other words, lack of any of the suggested tenets will be sufficiently capable to prevent a crime occurrence (Cohen & Felson).Other criminologists, namely Akers (2004) and Osgood et al. (1996) noted that routine activities theory suggests that most crimes are associated with the nature of an individual's daily routines based on sociological interrelationships; thus, illustrating that crime is based on situational factors which enable the criminal opportunities.Cyber space full of anonymity and impersonal as assumed thus termed as dis-inhibition and effort Suler,2004.Most crimes committed as per reports were by male about 94% and between the age of 15-40, Kigerl 2011, Higgins, Fell ad Wilson 2007.

OFFENDER + TARGET - GUARDIAN = CRIME

Offender reacts when feels target is suitable and guardian is absent (Akers and Sellers,2004) Acceptable guardian can just do anything (Cohen and Felson,1979).

Application of Sentimental Analytics with twitter

By using the tool of sentimental analytics, an analysis is made to identify global perspective on cyber crime and relevant security measures. Twitter Is used as a base for the same and the results are provided for the same. Sentimental analytics target to undersatand the view points or expression of users via twits across globe. Thus helps to map the results based on emotions such as anger, love, joy, happy, peace, disappointed and many more. Thus is proved to be one of the latest trends to identify the user's emotions for a product or service. Implementation of same in the study is helping to simply the most discussed term on one of the platforms of social media that is twitter. The coding for the same is done through "R" which is a tool used for data analytics and thus helps to understand global patterns on the term cyber space / security or threats.

Coding

```
install.packages("RColorBrewer")
install.packages("tm")
install.packages("wordcloud")
install.packages('base64enc')
install.packages('ROAuth')
install.packages('plyr')
install.packages('stringr')
install.packages('twitteR')
install.packages("tm")  # for text mining
install.packages("SnowballC") # for text stemming
install.packages("wordcloud") # word-cloud generator
install.packages("RColorBrewer") # color palettes
# Load
library("tm")
library("SnowballC")
library("wordcloud")
library("RColorBrewer")
library(RColorBrewer)
library(wordcloud)
library(tm)
library(twitteR)
library(ROAuth)
library(plyr)
library(stringr)
library(base64enc)
download.file(url="http://curl.haxx.se/ca/cacert.pem",destfile="cacert.pem")
requestURL <- "https://api.twitter.com/oauth/request_token"
accessURL <- "https://api.twitter.com/oauth/access_token"
authURL <- "https://api.twitter.com/oauth/authorize"
consumerKey <- "pBG65oqitBk630I42LsOe0JOh"
consumerSecret <- "tYabyp2jOrHiceEODxoGVYsHdnEX3TEQnNyUwZ41gT0pMt1IJH"
accessToken <- "3014467712-ugGnfOnhEjdNYyacxXSCq4y2QNlJnikbrUITIAk"
accessTokenSecret <- "JBWuJG03HEWLAahhMOZjA0gNJJhdYqJh6V3mhrfjAHewQ"
setup_twitter_oauth(consumerKey,
                    consumerSecret,
                    accessToken,
                    accessTokenSecret)
accessToken <- "3014467712-ugGnfOnhEjdNYyacxXSCq4y2QNlJnikbrUITIAk"

Objectname <- searchTwitter("cybersecurity", n=5000, lang=NULL)
df <- do.call("rbind", lapply(Objectname, as.data.frame))
write.csv(df,file = 'neww.csv')
fs<-df['text']

write.csv(fs,file = 'new.csv')
text <- readLines("C://Users/Naren/Documents/new.csv")
docs <- Corpus(VectorSource(text))
```

```
inspect(docs)
toSpace <- content_transformer(function (x , pattern ) gsub(pattern, " ", x))
docs <- tm_map(docs, toSpace, "/")
docs <- tm_map(docs, toSpace, "@")
docs <- tm_map(docs, toSpace, "\\|")
# Convert the text to lower case
docs <- tm_map(docs, content_transformer(tolower))
# Remove numbers
docs <- tm_map(docs, removeNumbers)
# Remove english common stopwords
docs <- tm_map(docs, removeWords, stopwords("english"))
# Remove your own stop word
# specify your stopwords as a character vector
docs <- tm_map(docs, removeWords, c("uuuu","eduubdedubu","https","via","amp"))
# Remove punctuations
docs <- tm_map(docs, removePunctuation)
# Eliminate extra white spaces
docs <- tm_map(docs, stripWhitespace)
# Text stemming
# docs <- tm_map(docs, stemDocument)
docs <- tm_map(docs, removeWords, c(""))
dtm <- TermDocumentMatrix(docs)
m <- as.matrix(dtm)
v <- sort(rowSums(m),decreasing=TRUE)
d <- data.frame(word = names(v),freq=v)
head(d, 10)
d<-d[-1,]
d<-d[-1,]
png("cybersecurity.png", width=12, height=8, units="in", res=300)
wordcloud(d$word, d$freq,min.freq = 40, random.order=FALSE, colors=brewer.pal(8, "Dark2"))
dev.off()
```

Figure - Mapping of Sentimental Analytics

The mentioned mapping result of **5000 users** across globe of **Twitter** who twits on same (results dated 26 February 2018) depicts that based on the emotional analytics that is **sentimental analytics,** infosec, iot, cyber are the most used terms or workds which are discussed the most on

social media platform. Where as the words such as capability ., generations, technology, worry, blockchian, quantum, bitcoin are the next discussed and followed by smart city, awareness, challenges, big data, malware, cyber crime, crypto currency, cyber attacks, threats, hackers, fintech and some more are the next to be discussed. Thus this shows the global concern regarding the cyber crime and security measurements related to same. Thus imparting the same supports the study to also know a real time situation when it comes to cyber security and related awareness.

Recommendations

Some of the major points to be noticed are:

1. Need for a Board approved Cyber-security Policy.
2. Cyber Security Policy to be distinct from the broader IT policy / IS Security Policy of a bank
3. Arrangement for continuous surveillance
4. IT architecture should be conducive to security
5. Comprehensively address network and database security
6. Ensuring Protection of customer information
7. Cyber Crisis Management Plan
8. Cyber security preparedness indicators
9. Sharing of information on cyber-security incidents with RBI
10. Supervisory Reporting framework
11. An immediate assessment of gaps in preparedness to be reported to RBI
12. Cyber-security awareness among stakeholders / Top Management Board
13. Setting up of Cyber Security Operation Center (C- SOC)

Conclusions

A variety of suggestions from delphi method were also received from Cyber lawers, Solution providers and Cyber cell experts. Also many suggestions were welcome such as rewarding ethical behavior, transparency in practices and ethics training, spread of awareness and cyber literacy, cyber security awareness programs, educating customers / users about trends in transactions, inventing new ways to design simple user friendly guidelines, awareness about cyber law and increasing know how regarding security measurements. For banks adoption of full proof method to ensure security.

A check was done to see whether the respondents used in the study really does use the online modes of financial transactions and expert advice were taken from cyber lawyers, cyber cell experts, bankers and solution provides. Interestingly the financial institutions included in the study are renounced one as the location being commercial hubs. With the digitization and demonetization there is a great digital development in the financial sector and the processes of digital financial transactions. India being the 12th nation to adopt cyber security measures abut still lot of gap is present when it comes to customer awareness for the same. India with a rapid pace is moving towards digitization and is one of the first to be called as digital economy across globe. With the adoption of recent trends in technology or involvement of digital blend in the financial sector, our nation needs to be equally paying attention towards awareness of cyber literacy across the country. The study is useful to all who are with the online process of financial transactions and thus must follow guidelines while practicing so. Lots of awareness aspects to be taken care of to educate users for financial transactions carried online.

There had been limited empirical work in the area of cyber security and customer awareness in terms in these locations of the study.

Bibliography -

[1] Arora K. (2003), 'Indian Banking: Managing Transformation through IT', IBA Bulletin, Volume 25(3), March, pp 134-38

[2] An Investigation of Financial Fraud in Online Banking and Card Payment Systems in the UK and China by Yan Sun, Loughborough University May 2010.

[3] Adv B Gordon Computer Crime – An Introduction (2002) February Servamus 35.

[4] Ahmad, Tabrez, New Begining of Cyberlaw in India (July 29, 2009). Available at SSRN.

[5] After Websites, Anonymous India to Hit Streets Against Cyber Laws,By Manoj Kumar.International Business Times, June 9, 2012.

[6] AshishPande, Deviation and Prevention, 2006, p. 126.

[7] An Explorative Study of Satisfaction Level of Cyber-Crime Victims with Respect to E- Services of BanksJournal of Internet Banking and Commerce, Vol. 17, No. 3, 2012 Dr.AtulBamrara ,Gajendra Singh Chouhan ,Mamta Bhatt.

[8] Bharti, Dr. Dalbir, Police and People – Role and Responsibilities, APH Publishing Corporation, New Delhi, 2006.

[9] Bayley, David H., "Community Policing", SardarVallabhbhai Patel Memorial Lectures (1984-2004), SVP National Police Academy, Hyderabad, 2005.

[10] Brynjolfsson Erik (1993) "The Productivity Paradox of Information Technology", Communication of ACM, Vol. 36(12),p.67-77.

[11] Brynjolfsson, Erik, Hitt, Lorin (1996) "Paradox lost? Firm-level Evidence on the Returns to Information Systems Spending", Management Science, April, Vol.42 No.4, p.541-558.

[12] Business Standard, Mumbai Police fall prey to cyber crime, Salary accounts with AXIS bankhacked, Sanjay Jog & Krishna Pophale | Mumbai June 14, 2013.

[13] Byte by Byte, cybercrime.planetindia.net, Gopika Vaidya-Kapoor, The Cyber Regulations Appellate Tribunal, February 18, 2003.

[14] Chopra V. K. (2006), 'IT and Business Process Re-Engineering', Indian Bankers – Special Issue on e-payments and Commerce, Volume 1(3), March.

[15] Chakravarthy, S.K., "Social Acceptability of the Police", The Indian Police Journal, Vol. XXVI, No. 1, July-September, 1979, p.3.

[16] Christopher D Chen Computer Crime and the Computer Fraud and Abuse Act of 1986 (1990) Computer Law Journal Vol. X No. 1 79.

[17] Choudhary, J.N., "Indian Police Leadership – Can it meet the Challenges of 21st Century", SVP National Police Academy Journal, Vol. 52: No. 2, July-December 2000.

[18] "China blames US and India for Cyber Attacks", *The Hindu*, August 11, 2011, p. 20 "Cyberabad Police to Roll out Host of New Measures", Staff Reporter, The Hindu, January 02, 2009.

[19] Centre Of Excellence For Cyber Security Research And Development In India(CECSRDI), Cyber Security Research And Development Centre Of India (CSRDCI) ,May 10, 2013.
[20] Cyber laws: Loopholes aplenty, PriyankaJoshi,Business Standard, Mumbai November 18, 2011. [40]
[21] Cybercrime now 'number one' threat: Europol chief,Agence France-Presse , 20April 2015, Indian Cyber Crime Centre.
[22] CyberLawIndia.Net.
[23] The Menace of Cyber Crime, Anusuya Sadhu, http://www.legalserviceindia.com/articles/article 2302682a.htm.
[24] Offences & Penalties under the Information Technology Act, 2000,Pradnya Pahurkar,Law Professor,November 17, 2010.
[25] Police minister announces plan to combat cyber-crime, eyewitness news, shamiela fisher , 2014.
[26] Reliance Capital files complaint against fake website, Press Trust Of India , 3 June 2013.
[27] Reserve Bank of India. (1984). Report of the Committee on Mechanisation in Banking Industry.
[28] RBI (1989) Report of the committee on computerisation in banks (The Rangarajan committee) Mumbai: Reserve Bank of India.
[29] RBI (1998) Report of the committee on Banking sector reforms (The Narasimhan committee) Mumbai : reserve bank of India.
[30] 'Ransomware' hits 150 PCs at Maha Mantralaya**,** Sujit Mahamulkar & Savio D Souza|, Times of India ,May 26, 2016**.**
[31] Retailers prepare for cybercrime offensive, OurWindsor.Ca, Michael Lewis, Oct 24, 2014.
[32] Rising cyber crimes have magnified challenges: Rajnath Singh, Press Trust of India, The Indian Express, Hyderabad , October 31, 2014.
[33] Mace, A. E. (1964), Sample-size determination, Reinhold, New York.
[34] Kraemer, H. C. and Thiemann, S. (1987), How Many Subjects? Statistical Power Analysis in Research, Sage Publications, Newbury Park, CA.
[35] Cohen, J. (1988), Statistical Power Analysis for the Behavioral Sciences, Academic Press, New York, 2nd edn.
[36] Desu, M. M. and Raghavarao, D. (1990), Sample Size Methodology, Academic Press, Boston.
[37] Lipsey, M. W. (1990), Design Sensitivity: Statistical Power for Experimental Research, Sage Publications, Newbury Park, CA.
[38] Shuster, J. J. (1990), CRC Handbook of Sample Size Guidelines for Clinical Trials, CRC Press, Boca Raton.
[39] Odeh, R. E. and Fox, M. (1991), Sample Size Choice: Charts for Experiments with Linear Models, Marcel Dekker, New York, second edn.
[40] Freiman, J. A., Chalmers, T. C., Smith, Jr., H., and Kuebler, R. R. (1986), "The Importance of Beta, the Type II Error, and Sample Size in the Design and Interpretation of the Randomized Controlled Trial: Survey of 71 "Negative" Trials," in Medical Uses of Statistics, eds. J. C. Bailar III and F. Mosteller, chap. 14, pp. 289–304, NEJM Books, Waltham, Mass.
[41] Thornley, B. and Adams, C. (1998), "Content and quality of 2000 controlled trials in schizophrenia over 50 years," British Medical Journal, 317, 1181–1184.
[42] The 5 financial secrets you should never reveal, Vivina Vishwanathan, Mint Mumbai, 1/8/2017.
[43] Information is gold and it can be robbed and stolen, Mumbai Mint, Personal Finance (12,) 26/7/2017.