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), Bradward W. Reys (2012), E. Gabriella (2012), Jean, , Brody, Richard G.; Mulig, Elizabeth; ; Redsins (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 advances 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). Flanagan and McMenamin (1992) state computer Crime-committed by new generation of hackers might cost cybercrime victims, as a collective, anywhere from $500 million to $5 billion a year. The Computer Emergency Response Team Coordination Center (CERT/CC) reports that "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); theft (including theft of personal information and identification-related data); and 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 role 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, & Bonatti, 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 understand 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("RCColorBrewer")  # color palettes

# Load
library("tm")
library("SnowballC")
library("RCColorBrewer")
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 <- "tYabyp2jOrHiceEODxoGVYsHdnEX3TEQnNyUwZ41gT0pMt1JH"
accessToken <- "3014467712-ugGnfOnhEjdNYyacXXScqy2QNJiikbrUITIAk"
accessTokenSecret <- "JBWuJG03HEWLAaahhMOZjA0gNJJhdYqJh6V3hrfjAhewQ"
setup_twitter_oauth(consumerKey, consumerSecret, accessToken, accessTokenSecret)

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 lowercase
docs <- tm_map(docs, content_transformer(tolower))
# Remove numbers
docs <- tm_map(docs, removeNumbers)
# Remove English common stop words
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 words which are discussed the most on
social media platform. Where as the words such as capability .., generations, technology, worry, blockchain, 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 lawyers, 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 providers. Interestingly the financial institutions included in the study are renowned 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 of these locations in the study.

**Bibliography**

Centre Of Excellence For Cyber Security Research And Development In India (CECSRDI), Cyber Security Research And Development Centre Of India (CSRDCI) May 10, 2013.


Cybercrime now 'number one' threat: Europol chief, Agence France-Presse, 20 April 2015, Indian Cyber Crime Centre.

CyberLawIndia.Net.


Reliance Capital files complaint against fake website, Press Trust Of India, 3 June 2013.


‘Ransomware’ hits 150 PCs at Maha Mantralaya, Sujit Mahamulkar & Savio D Souza, Times of India, May 26, 2016.


Raising cyber crimes have magnified challenges: Rajnath Singh, Press Trust of India, The Indian Express, Hyderabad, October 31, 2014.


The 5 financial secrets you should never reveal, Vivina Vishwanathan, Mint Mumbai, 1/8/2017.

Information is gold and it can be robbed and stolen, Mumbai Mint, Personal Finance (12,) 26/7/2017.