(IJRST) 2016, Vol. No. 6, Issue No. IV, Oct-Dec **e-ISSN: 2249-0604, p-ISSN: 2454-180X**

WHITE-COLLAR CRIMES: AN ALARMING TREND

Raghav Mittal

Improvement or advancement, in any perspective, means to improve, no matter how small it is, a system. Betterment is a basic process to improve the system than what it presently is rather than to remove all the shortcomings present. The subject of white-collar crimes and its eradication is a good way to understand the topic of betterment truly. In simple words, white-collar crimes are offences that are punishable by law because these felonies affect individuals or organizations financially (loss of financial resources) or socially (loss of reputation). The list of white-collar crimes has been increasing exponentially over the past few years, whether it be Edward Snowden oozing National Security Agency's classified information (Leith, Bengali and Cloud) or it be Mr. Belfort operating a boiler room as a penny stock scam. But the felonies that has been the primary concern for the security agencies all over the world is Cybercrime, which is executed using networks and computers. According to the article, "U.S Agency to Combat Cyber Threats", by Paresh Dave states, "Cyber attacks are draining as much as $140 billion and half a million jobs from the U.S. economy each year." There is an immediate need to take serve steps in order to reduce cyber crime and punish the organizations or the individuals that are responsible behind it. However, computer crime is partly due to the negligence of the common man, who log's in online and carelessly enters his or her information on whatever web application he is presented with. There have been several attempts by various companies and security agencies to eradicate cybercrime, but all efforts will go in vain unless the common people follow some basic practices to protect themselves from the felony. Henceforth, the common man should be more cautious with his private information and should be educated through social media that people should be more prudent while sharing their private information online or on any unknown web application.

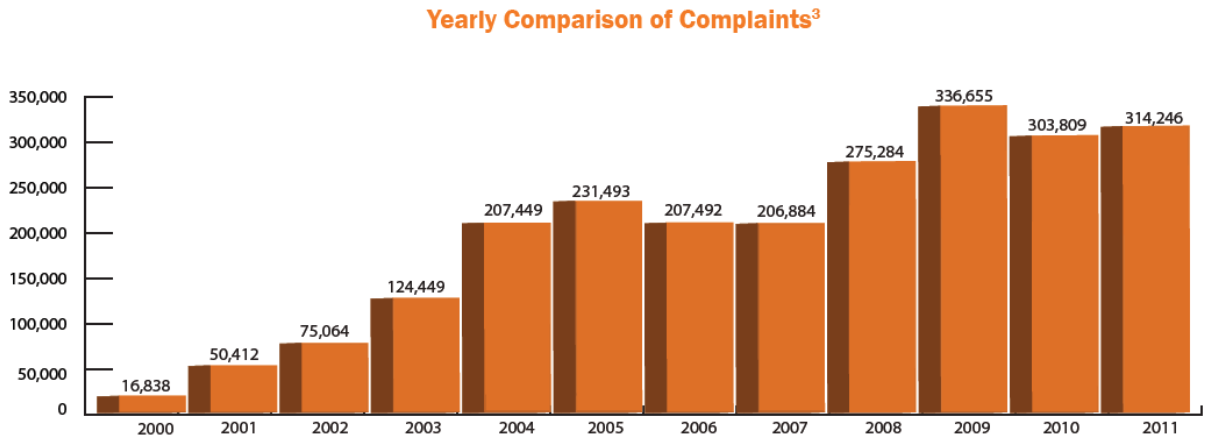

Figure 1. Yearly complaint comparison from 2000-2011. Data collected from '2011 IC3 – Internet Crime Report'

On May 8, 2000, the partnership between The Federal Bureau of Investigation and The National White Collar Crime Center(NW3C) was named, The Internet Crime Complaint Center (IC3), which is primarily responsible to address and fight all the cybercrime practices around the world (Pfeifer). Fig. 1 clearly depicts the increasing number of complaints registered by the individuals who have been affected by cybercrime over the span of 10 years. The research study, "MONDAY BUSINESS; Internet Fraud's U.S. Price Tag Put at $550 Million; the Toll Doubles from 2008 as People Fall Prey to Increasingly Sophisticated Scams", published in *The Los Angeles Times* by Stuart Pfeifer states, "In 2011, the center received over 300,000 complains with an estimated loss of over $550 million." The common notion of white collar crimes only being associated with large corporations, governments, or wealthy individuals is both wrong and deceiving. The potential target for any hacker can be as big as President Barack Obama or can be as small as a high school student. What if someone were to upload your Facebook messenger conversations online? What is someone were to steal all your money from your bank account? What if someone were to put your all your financial details on the web? What if someone were to hack your social networking account and steal your identity? As mentioned earlier, even the common man can be at risk and be prone to the above stated situations. Therefore, precluding web crime should be of utmost importance for governments and security agencies from all around the globe.

Measures to fight cybercrime have been recorded since the first major reported cases, but has done no good. According to the newspaper report, "Rethinking Banking Rules", by Gary Warner, one of the highest reported banking cybercrime occurred in 1970, when New York Union Dime Savings Bank's chief teller embezzled around 1.5 million USD from several bank accounts at the Park Avenue branch. Adding more to the list of computer crimes, in 1983, a

student at UCLA used his computer skills to hack the Defense Department's international communication system (Stewart). The above mentioned cybercrime examples not only portray the prolong history of white-collar crime, but also displays the troublesome experience that government agencies and wealthy companies have in order to stop and identify internet criminals in a timely manner. The situation gets no better today, in 2012, gigantic multinational companies like LinkedIn and eHarmony were compromised with 65 million password hashes (Hsu). The newspaper article, "Hacker Hits Shoe Retailer Zappos.Com; Full Credit Card Numbers Were Not Exposed in the Cyber Attack, the Firm Says", published in *The Los Angeles Times* states another high profile cyber case where the credit card and personal information of about 24 million customers were compromised because of the security hack at Zappos.com (Chang). There have been no significant initiatives by organizations in order to eradicate cyber crime, which today is not so difficult with increasing security technologies, and result in spending a vast amount of financial resources in order to regain from the breaches.

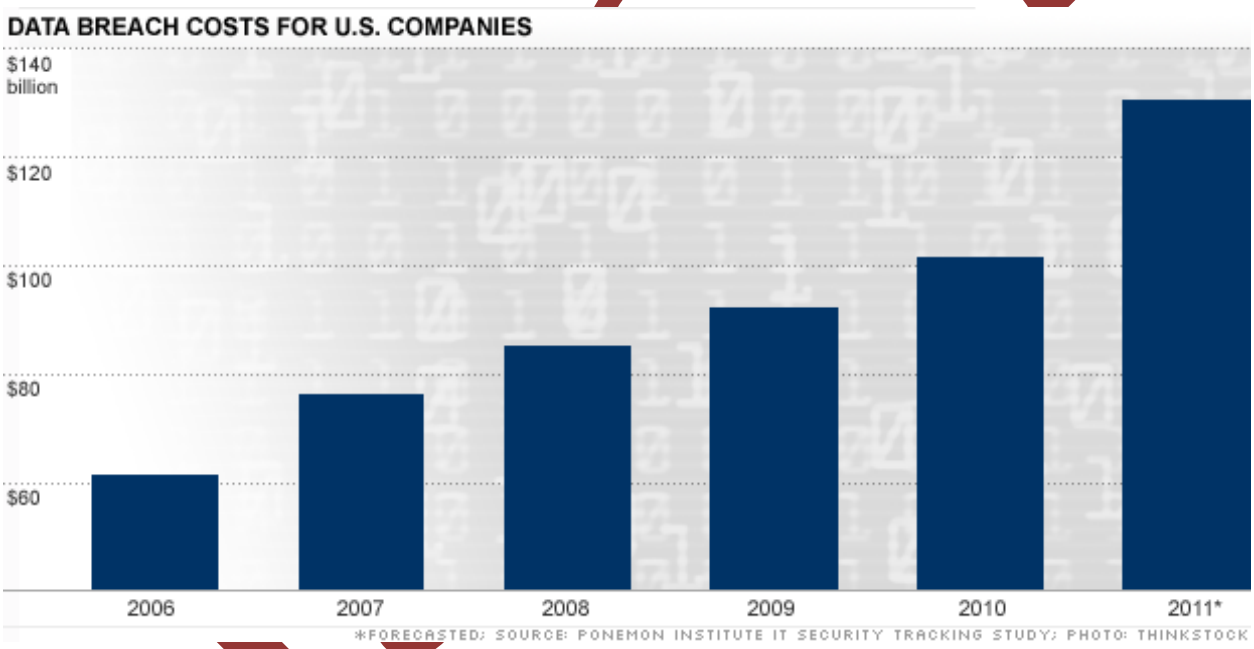

Figure 2. Yearly data breach costs comparison for US companies, from the year 2006 - 2011. Data collected from, 'The Cost of Cybercrime – MONEY.CNN.COM'

The numerous measures by companies and individuals to fight against cyber-crime is costing them millions of dollars each year. Fig. 2 clearly illustrates the "price tag on corporate data breaches is soaring" (Goldman). According to a cyber security research organization, Ponemon Institute, in the year 2011, an average of about 29 million USD was spent by several companies to recover from the aftermaths of the terror of cybercrime (Rodriguez). The amount

spent is huge and cannot be looked at and be disregarded easily. The money that could be used wisely in order to help and improve the American economy is now spent to fight against the activities of a few anti-social elements. On the concerning issue of increasing web crime, Larry Ponemon, the chairman of the Ponemon Institute, once commented, "The ability of bad guys to enter, steal, exit and do it in a way that's undetectable is rising. It's a big problem and it is getting worse" (Goldman). As always said, "precaution is better than cure", in my opinion, companies and organizations should charge some extra funds and keep it specifically to invest in web security. For example, corporate giants like Bank of America and Price Waterhouse Coopers have invested in a technological advance burglar alarm system, Counterpane Internet Security Inc. system, that costs them a whooping amount of 12,000 USD per month (Schneier). However, there have several incidents where the loss incurred by the individual is massive and cannot be measured in dollars.

One of the biggest cyber-crime event was recorded in December 2014 that left the Sony Pictures Entertainment shocked. The newspaper article, "COMPANY TOWN; ex-employees suing Sony over hack; two lawsuits seeking class-action status say the firm didn't protect workers' data", published in *The Los Angles Times* by James and Hamedy, has illustratively described the Sony systems hack. "The Sony Systems Hack, where the group, calling itself Guardians of Peace, demanding the cancellation of the release of *The Interview*, 'divulged data including thousands of emails from studio chiefs, salaries of top executives and Social Security numbers of 47,000 current and former employees.' Medical information of some employees and their family members was contained in the mountains of data the hackers posted on file-sharing sites" (Hamedy & James). Putting oneself in the victim's shoes is itself terrifying and the thought of having one's information open on the web is although more horrifying. The law team representing The Sony Entertainment Pictures have filled two different lawsuits in the city of Los Angeles that tend to obtain action-class status, "alleging Sony Pictures Entertainment was negligent in the months leading up to the devastating hack" (Hamedy & James)." In another words, the employees at Sony Entertainment are contemplating on the fact that it is the liability of the multi-billion-dollar company as they ignored the security warning's of their information system being vulnerable to hack. In addition to this, the employees are arguing that the government should delve deep into the matter and fine the company because it was their negligence that lead to the violation of the human right to privacy and victimized thousands of employees working in the organization. The Sony Hack is listed under one of the biggest cases of cyber-crime in 2014.

Another one to add more to the never ending list of cyber-crimes is the Celebrity photo hack in 2014. According to the newspaper report, "Alleged photo hack is probed; FBI, apple look into reports that nude celebrity images were stolen, posted online", published in *The Los Angeles Times*, "several photos of actress Jennifer Lawrence, circulated on various websites and social media platforms. A representative for Lawrence called the published photos a flagrant

violation of privacy." The same newspaper report also included a statement from Apple which said, "it was actively investigating reports that the photos were stolen from its iCloud service. Apple did not say whether its services, or celebrity iCloud accounts, were breached" (Khouri & Sahagun). Apple has to stand up for its shortcomings and their remaining shut on this given issue does no good. While on the other hand, it is inhuman for the hackers to carry out these activities just for the sake of their entertainment and incidents like these can become nightmares for the victims causing them mental, emotional, and social distress. The best plausible way to mitigate such acts, where the employees or the users end up becoming the center of mockery, is either to implement a security software that imposes restriction on the user to upload any offensive stuff on the internet or to encode private data such as medical records and social security number. There have been several efforts by software professionals all around the globe to implement such kind of security software (O'Brien). Tiffany Hsu's newspaper article, "COMPUTERS; Intel in Deal to Acquire McAfee; the Purchase Could Allow the Firm to Put Anti-Virus Technology Directly into its Chips", states that cybercrime and its associated effects may scoop down by 39% once these security anti-cybercrime software is developed. Such web safekeeping softwares might go a long way to end victimization due to the reduced rates of cybercrimes, but surely will not eradicate the risk posed by the web terrorists.

Cyber criminals or cyber terrorist is a group of people that countries and organizations around the world are trying to shut down. The article, "Terrorists 'gaining upper hand in cyber war'", by Kim Sengupta states,"Cyber eliminates the importance of distance, is low cost and anonymous in nature, making it an important domain not just for hostile states, but terrorists and criminals." To rephrase, cyber attacks have been increasing in number over the past few years because it does not require large infrastructure or resources, is easy to execute, and usually has no risk of death involved for the terrorist organization.Since cyber criminals function at the highest level of anonymity, web terrorists are capable of instigating a cyber war with a few finger movements here and there over the keyboard. *Fire Sale* is one of the most dangerous forms of cyber warfare attack, where the web terrorists perform a three-staged attack on the National Computer Infrastructure. The first stage includes the shutting down of all the transportation systems, for example, railroad lines, traffic lights, subway and airport systems. The second stage includes the disabling of the financial systems across the nation, such as Wall Street, banks, and other financial institutes. The final stage three includes the turning off all the public utility systems, such as, electricity, gas pipe lines, satellite systems, and telecommunications. All the above mentioned stages include everything that a common man makes use of on an everyday basis.The given process of Fire sale may seem difficult at first, but it is surely not impossible with the technological advancement we have in today's generation. Therefore, it is the need of the hour to bring these cyber criminals, who are capable of instigating such overwhelming tasks, to justice.

(IJRST) 2016, Vol. No. 6, Issue No. IV, Oct-Dec **e-ISSN: 2249-0604, p-ISSN: 2454-180X**

The idea of reducing white-collar crimes has become even more predominant due to the world happenings, both in the past as well as in the present. Barack Obama, in one of his interviews, once said, "America's economic prosperity, national security and our individual liberties depend on our commitment to securing cyberspace and maintaining an open, interoperable, secure and reliable Internet" (Hennessey).The legislature is doing its job by passing laws such as *Improving Infrastructure Cyber Security*- 13636 to eradicate the risk of cyber crime. These measures have been taken in the past by the administration but did no good due to the hostility from the private institutions and due to the lack of financial funds and manpower (Parsons). However, over the past few years, private organizations, especially corporate giants like Microsoft, are taking initiatives to make the virtual cyberspace secure. By uniting the multi-national companies together, The Cybercrime Center focusses primarily on piracy, digital crimes and intellectual property theft. Lastly, it is not only the responsibility of the legal administrative bodies but also the responsibility of the common man to eradicate or reduce the rate of cyber-crime. Individuals should make sure to neither indulge in any form of cybercrime nor become its victim.

One of the easiest platforms to perform cyber crime is social media, especially Facebook. The research study, "Friend or cyber criminal? Cybercrime growing on Facebook",by J. Finkle states, "Cybercrime is rapidly spreading on Facebook as fraudsters prey on users who think the world's top social networking site is a safe haven on the Internet." However, managing millions of new accounts each day, Facebook is correct in saying, "we do our best to keep Facebook safe, but we cannot guarantee it" (Finkle) and cannot be made liable for the cyber crime activities. Despite of the continuous update by the corporations to guard their users from cyber criminals, most of the time the corporations loose the race. It is the duty of the user to be careful and effective while using the social networking services, such as to make sure who they are talking to while they are online. For instance, it may not be a bad idea to cross-check the mutual friends before accepting a friend-request on a social networking site like Facebook.

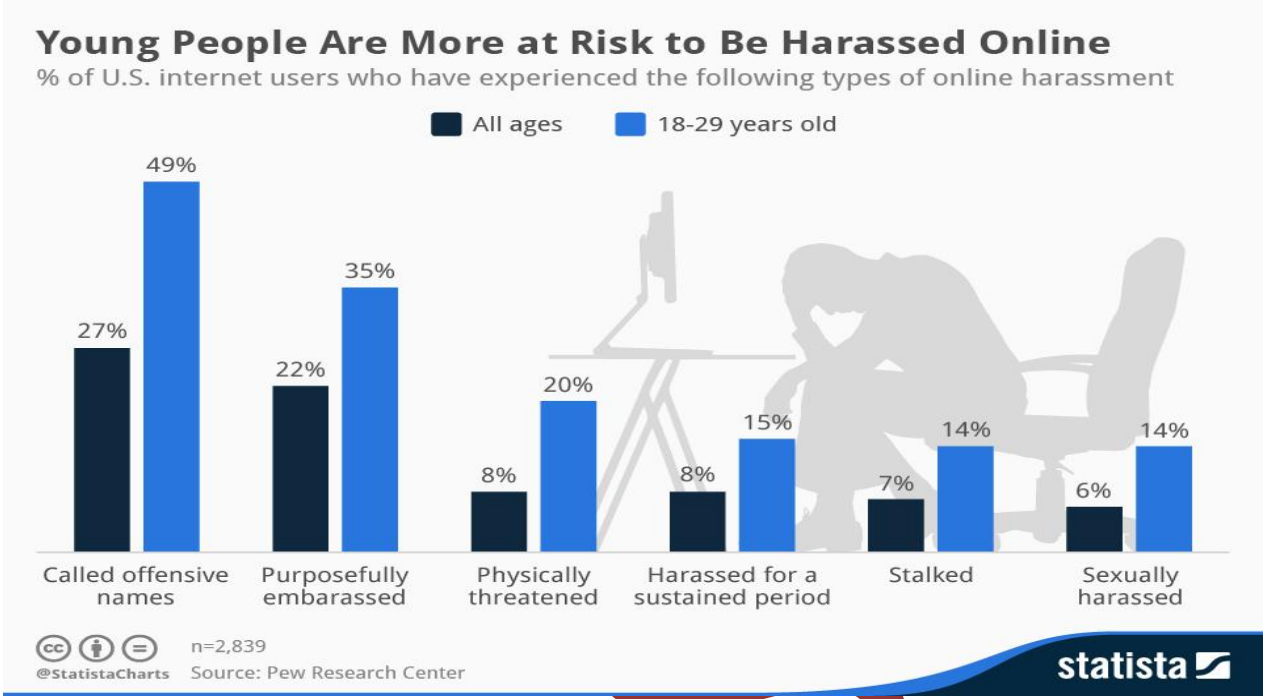

Figure 3. Young people are at more risk to be harassed online. Data collected from 'StatistaCharts.'

Cyber-Bulling, is another form of cyber crime, the effects of which are far more than loss of financial resources. In simple words, Cyber Bulling refers to the deliberate pestering of an individual by using Information Technology as a resource. The above included, Fig. 3 clearly illustrates to the fact that young teens are more prone to the wrath of cyberbullying. The graph represented in Fig. 3 shoes how people from different age groups are target to different forms of cyber-crime. The newspaper article, "Bullies' new playground is cyberspace; online bullying has become the latest and most pervasive method of meanness toward teens", by K. Sudol states,"Cyberbullying has become the latest and most pervasive method of meanness in the already tough world of teens." Harassment, threatening or humiliating of peers are some of the examples for which computers, cellphones, and social networking sites can be used to great effectiveness. In his article, Sudol also mentioned, "According to the U.S. Department of Education, more than 900,000 secondary students reported being cyberbullied in 2007." The day to day technological advancements and the extensive reach of the internet world is what makes this evil practice of cyberbullying so pernicious. The harassment and bullying at the school and university levels gained intense attention after the suicide case of Tyler Clementi, a freshman at the Rutgers University. After Clementi's roommate streamed a video of his intimate gay encounter on the web, Tyler Clementi jumped to his death from the George Washington bridge

(Susman). Children and teenagers who indulge in these activities do not realize the fatal effect cyberbullying has on the victim.

The wrath of cybercrime cannot be combated in a single day but measures have to be taken over time to fight against it. “Atty. Gen. Eric H. Holder Jr. and FBI Director James Comey have repeatedly warned that cybercrime poses one of the gravest threats to the U.S.” (Serrano). According to the present scenario, the government is the one who is potentially undertaking all the responsibility to mitigate cybercrime and its criminals. In one of their newspaper articles, Brian Bennett and Paresh Dave, stated, “The Obama administration recently announced plans to create a cyber intelligence center to better respond to digital breaches and threats to federal agencies and private industry.” The question that arises here is whether the common man is also willing to work towards the same goal. The article, “TECH SAVVY; how to Safeguard Your PC from Hackers”, by David Sarno states a few ways that we can protect ourselves from cyber crime, some of them being, “Watching what you put into your computer is paramount. Avoid downloading programs from the Internet, opening strange email attachments or visiting unfamiliar websites. Those are the most common modes of infection.” Another way to combat cyber crime is report. As soon as you discover that something is fishy or is not right, report it. Sites like Facebook have services with which you can report suspicious events with one click on the mouse. While accessing financial and personal details, users should make sure about the minutest of the trivial details. Banks, for example, have started implementing unique identification patters and keys on their websites, which is a way that can be used to authorize that it is a legitimate site or banks today have started using on-screen keyboards that reduce the chances for the hackers to track the user password. It is to no avail for the corporations to spend millions of dollars and make their computer architecture systems secure and strong enough to respond to cyber threats unless and until the individuals take cautious steps to protect themselves from the horror of cyber-crimes.

WORK CITED:

Bengali, Shashank, and David S. Cloud. "Bent on Shining a Light on U.S. Security; as an NSA Contractor, Edward Snowden Evolved into an Ardent Proponent of Civil Liberties." *Los Angeles Times.* Jun 11 2013.

Bennett, Brian, and Paresh Dave. "U.S. Agency to Combat Cyber threats; the Operation Will Analyze Intelligence, Fight Digital Attacks on Government, Industry." *Los Angeles Times.* Feb 11 2015.

Chang, Andrea. "Hacker Hits Shoe Retailer Zappos.Com; Full Credit Card Numbers were Not Exposed in the Cyber Attack, the Firm Says." *Los Angeles Times.* Jan 17 2012.

Dave, Paresh. "Study Finds Lower Cost of Cybercrime." *Los Angeles Times.* Jul 23 2013.

Dixon, Robyn. "COLUMN ONE; 'I Will Eat Your Dollars'; to the Cyber Scammers in Nigeria Who Trawl for Victims on the Internet, Americans are Easy Targets. But One Thief had Second Thoughts." *Los Angeles Times.* Oct 20 2005.

Drogin, Bob. "In Theory, Reality, U.S. Open to Cyber-Attack; Security: An NSA Test Exposed Vulnerability of Critical Computer Systems to Hackers. Outside Assault proved it." *Los Angeles Times*: 16. Oct 09 1999.

Finkle, J. "Friend or cyber criminal? Cybercrime growing on Facebook." *The Globe and Mail.* Jul 01 2009.

Goldman, David. "The Cost of Cybercrime." *Money.cnn.com.* 22 July 2011.

Hamedy, S., & James, M. "COMPANY TOWN; ex-employees suing Sony over hack; two lawsuits seeking class-action status say the firm didn't protect workers' data." *Los Angeles Times.* Dec 17 2014

Hart, Michael. "Privacy in Cybercrimes Promised." *Los Angeles Times.* Nov 01 2002.

Hennessey, Kathleen, and Chris O'Brien. "Ways to Protect Data are Unveiled; White House Releases Voluntary Guidelines for Companies to Fend Off Cyberattacks." *Los Angeles Times.* Feb 13 2014.

Henrigan, W. J. "Hackers for Hire; Faced with Increasingly Sophisticated Technology Threats, Boeing and Other Defense Contractors are Employing Computer Geeks to Boost Cyber Security." *Los Angeles Times.* Apr 15 2012.

Hsu, Tiffany. "Barnes & Noble Says its Stores were hacked; Thieves may have Stolen Customer Data by Planting Bugs at 63 Outlets Nationwide." *Los Angeles Times.* Oct 25 2012.

Hsu, Tiffany. "COMPUTERS; Intel in Deal to Acquire McAfee; the Purchase could Allow the Firm to Put Anti-Virus Technology Directly into its Chips." *Los Angeles Times.* Aug 20 2010.

Huck, Joe. "BUSINESS BRIEFING; CYBERCRIME; Europeans Shut Down Hackers." *Los*

Angeles Times. Feb 26 2015.

Iritani, Evelyn. "Thailand Plans a Fire Sale; Asia: In another Step Toward Recovery, Nation Will Auction $10 Billion in Loans. The Prospect of Foreign Investors Playing such a Huge Role in its Economy Troubles Many Thais." *Los Angeles Times*: 1. Nov 14 1998.

Khouri, A., & Sahagun, L. "Alleged photo hack is probed; FBI, apple look into reports that nude celebrity images were stolen, posted online." *Los Angeles Times.* Sep 02 2014.

Kim Sengupta, D. C. "Terrorists 'gaining upper hand in cyber war'." *The Independent.* Feb 06 2010.

Leith, William. "Penny-Stock Profiteer Turns Witness; Securities: Former Boiler-Room Chief Who may have Bilked $200 Million from Investors Testifies Against Ex-Colleague." *Los Angeles Times*: A18. Oct 30 2000.

Li, Shan. "Home Depot Breach Larger than Target's; the Hardware Chain Says about 56 Million Payment Cards were Exposed in Massive Cyberattack Last Year." *Los Angeles Times.* Sep 19 2014.

Memoli, Michael A., and Ryan Faughnder. "New Action Targets North Korea; U.S. Officials Dismiss Experts Who Say no Evidence Proves the Country's Involvement in the Sony Hack." *Los Angeles Times.* Jan 03 2015.

Morrison, Patt. "PATT MORRISON ASKS | DOUGLAS THOMAS; the Hacking." *Los Angeles Times.* Dec 24 2014.

O'Brien, Chris. "New Cybersecurity Boom Arrives in Silicon Valley." *Los Angeles Times.* Dec 06 2013.

Parsons, Christi, and Kathleen Hennessey. "Obama Seeks Help on Cybersecurity; He Calls for a 'Spirit of Collaboration' between Government and the Private Sector." *Los Angeles Times.* Feb 14 2015.

Pfeifer, Stuart. "MONDAY BUSINESS; Internet Fraud's U.S. Price Tag Put at $550 Million; the Toll Doubles from 2008 as People Fall Prey to Increasingly Sophisticated Scams." *Los Angeles Times.* Mar 15 2010.

Rodriguez, Salvador. "Cyber Crimes Get More Costly; the Median Tally of such Attacks for a

Company Per Year Rises to $5.9 Million." *Los Angeles Times.* Aug 03 2011.

Sarno, David. "TECH SAVVY; how to Safeguard Your PC from Hackers." *Los Angeles Times.* Jul 17 2011.

Schneier, Bruce. "New Firm Opens Web Security Options; Internet: Counterpane, Whose Analysts Review Corporate Customers' Activity from Remote Sites, Offers an Alternative to in-House Monitoring." *Los Angeles Times*: 7. Apr 03 2000.

Serrano, Richard A. "Justice Department Steps Up Fight Against Economic Cyber spying." *Los Angeles Times.* Oct 22 2014.

Stewart, Robert W. "Hacker Who Tapped Defense Computers Faces Mental Testing." *Los Angeles Times*: 28. Aug 24 1985.

Sudol, K. "Bullies' new playground is cyberspace; online bullying has become the latest and most pervasive method of meanness toward teens." *Los Angeles Times.* May 22 2011.

Susman, Tina. "THE NATION; Guilty Verdict in Hate Crime Trial; an Ex-Rutgers Student Who Secretly Filmed His Gay Roommate is Convicted." *Los Angeles Times.* Mar 17 2012.

Tu, Janet I. "Microsoft Opens Center to Crack Down on Cybercrime." *Los Angeles Times.* Nov 30 2013.

Warner, Gary. "Rethinking Banking Rules." Business World. Jul 2013.