International Journal of Computer

(IJC)

ISSN 2307-4523 (Print & Online)

http://ijcjournal.org/

The Rise in Cybercrime and the Dynamics of Exploiting the Human Vulnerability Factor

Dr. Nabie Y. Conteh[a]*, Malcolm D. Royer [b]

[a] *Department of Computer Information Systems, College of Business & Public Administration Southern University at New Orleans, 6801 Press Drive, Suite 108, New Orleans, Louisiana 70126, USA*

[b] *Department of Cyber Security and Information Assurance, Graduate School of MGT and Technology University of Maryland University College Adelphi, Maryland, USA*

[a]*Email: nconteh@suno.edu*

[b]*Email: malcolm.d.royer@gmail.com*

Abstract

This paper is primarily intended to firstly define and review the literature in cybersecurity and vividly shed light on the mechanisms involved in the social engineering phenomenon. It will discuss the various attempts at network intrusion and the steps typically taken in the implementation of cyber-thefts. The paper will provide the rationale behind the justification of why humans are considered to be the weakest link in these attacks. The study will also explain the reasons for the rise in cybercrimes and their impact on Organizations. In closing, the paper will put forward some recommendations to serve as preventative measures and solutions to the threats and vulnerabilities posed by cyber-attacks. Finally, measures, such as conducting regular, thorough, and relevant awareness training, frequent drills and realistic tests will be addressed with a view to maintaining a steady focus on the overall discipline of the organization thereby hardening that component of the network that is the softest by nature—the human vulnerability factor.

Keywords: Social Engineering; Cybercrime; Cyber theft; Network Intrusions; Preventive Measures**.**

1. Introduction

The security of an organization is only as strong as its weakest component.

---

* Corresponding author.

In an era of increasing technological advances in the methods of conducting business, one might think that the security of those resources mostly lies in technical controls and programming algorithms. While the technical side of security is critically important, there is a vulnerability that cannot be removed by technological means. That vulnerability is unique to a particular element unavoidably necessary in the daily operation of any company. This indispensable component is the human employee, who is susceptible to attacks of a decidedly low-tech nature—social engineering.

2. Social Engineering

2.1 Definition

The term "social engineering" as it pertains to computer and network security is not new—it has been around since at least 1995 when Al Berg used it in his article "Cracking a Social Engineer" in LAN Times—but it has not yet made its way into all standard dictionaries. The 2015 editions of the Merriam-Webster, Random House, and Cambridge Free English dictionaries only define social engineering in terms of the social or political sciences, not security. Among the information security community, however, social engineering refers to "the practice of fooling someone into giving up something they wouldn't otherwise surrender through the use of psychological tricks" [2]. Curry goes on to state that social engineers "rely on the normal behavior of people presented with data or a social situation to respond in a predictable, human way" and explains that this kind of attack relies on "presenting trusted logos and a context that seems normal but is in fact designed to create a vulnerability that the social engineer can exploit" [2].

In his book Ghost in the Wires about his exploits as a hacker, Kevin Mitnick defines social engineering as "the casual or calculated manipulation of people to influence them to do things they would not ordinarily do" [10]. He gives a clear example of a typical method of obtaining unauthorized information as a part of his breaking into U.S. Leasing's computer network:

I would call the company I'd targeted, ask for their computer room, make sure I was talking to a system administrator, and tell him, "This is [whatever fictitious name popped into my head at that moment], from DEC support. We've discovered a catastrophic bug in your version of RSTS/E. You could lose data." This is a very powerful social-engineering technique, because the fear of losing data is so great that most people won't hesitate to cooperate [10].

Accurate as this example is, it only depicts one aspect of social engineering: pretexting—setting the conditions (a story, subtle or explicit clues, name-dropping, internal buzz-words and terminology, etc.) for a victim to believe that the attacker comes from a legitimate background. The other forms of attack that fall under the classification of social engineering, including the definitions pit forward in this article are:

- Baiting—leaving Trojan horse style equipment or software lying in the open with an enticing title or appearance as bait.
- Phishing—using a scam email to deceive a victim.
- Piggybacking (or tailgating)—following someone into a secure environment, with or without them

detection.

- Quid Pro Quo—giving someone something in return; exploiting a person's goodwill.
- Shoulder Surfing—watching someone enter knowledge-based credentials and remembering them for future unauthorized use.
- Vishing—using an interactive voice response system to trick a victim into inputting personal information over the phone.

According to [5], regardless of the specific attack method, the basic methods of persuasion used are "impersonation, ingratiation, conformity, diffusion of responsibility, and plain old friendliness….the main objective is to convince the person disclosing the information that the social engineer is in fact a person that they can trust" [5]. An additional supplement to the information-gathering process and development of a plausible background prior to pretexting is dumpster diving—sifting through discarded files for sensitive information.

3. Role in Network Intrusion and Cyber Theft

Social engineering plays a major and enduring role in network intrusion and cyber theft. This is not to say that it is an absolutely necessary role, as a cracker could conceivably infiltrate a system without any human interaction through exploiting technical vulnerabilities. The significance of the role that it plays is due to the ongoing vulnerability any system has and will continue to have—its users and administrators.

3.1 Humans are the weakest link

Because people are involved in the management and use of any computer network, they will always have to be considered one of the links to the security chain. This link is and will continue to be the weakest for the simple reason that people are easy to manipulate. We are subject to emotions that frequently override any commitment to logic that we may have. We have a psychological dimension that computers, which are based upon pure, straightforward logic, do not have. Our psychological weaknesses and needs, coupled with our faulty memory and flighty attention span, leave us highly vulnerable to deception and emotional manipulation.

Dr. George Simon talks about successful psychological manipulation in his book *In Sheep's Clothing*, stating that it requires the manipulator to conceal aggressive intentions and behaviors, know the psychological vulnerabilities of the victim, and be ruthless enough to disregard any harm caused to the victim [13]. Since there is no psychological aspect to a computer's processing and intentions and behaviors are perceived in terms of analysis of a sequence of actions taken, these approaches would be irrelevant to a technical system were it not for the human component. According to Dr. Harriet Braiker in her book *Who's Pulling Your Strings?*, manipulators control their victims using positive and negative reinforcement, intermittent or partial reinforcement, punishment, and traumatic one-trial learning [1]. They play upon the desires that most people have for affirmation, affection, and appreciation while taking advantage of our natural tendency to want to help others, especially those who share an affiliation of some sort with us. These are all vulnerabilities that a computer, based in unyielding logic, is not subject to.

3.2 No technical expertise needed

Because it is independent of the technical controls in the systems used, social engineering attacks can be carried out with minimal specialized knowledge on the part of the attacker. There is no need for experience in computer programming or thorough understanding of the underlying network structure in order to steal critical information through a conversation with an employee. All that is needed is enough of a backstory to seem plausible, a good sense of timing, a basic knowledge of the power names and common internal terminology, and anyone can don the mantle of social engineer.

This vulnerability that organizations have to social engineering attacks will continue to exist for the foreseeable future regardless of how advanced our technological systems become, as long as people are involved in some way. We see this over and over again in depictions of a technologically hyper-advanced future society as seen in science fiction movies and TV shows. How often does the protagonist (and sometimes the antagonist) use low-tech, social interaction-based methods to bypass security systems?

4. Reasons for Rise in Cybercrime

It is difficult to obtain accurate numbers detailing the steady increase of cybercrime throughout the globe as the statistics are built on numbers of attacks, breaches, and other security events that are reported, leaving unreported numbers unaccounted for. However, CNN Money cites a report by Ponemon Institute that claims 47% of adults in the United States alone have had their personal information exposed, with 110 million of these data breaches occurring over a 12-month period from May 2013 to May 2014 as cited in [11]. A world statistics portal reports that two of the most well-known companies suffering data breaches, Adobe and eBay, had 152 million and 145 million records stolen as of August 2015 [14]. There are two major reasons for this rise in cybercrime over the last decade: the low risk and relative safety for attackers; and the increasing targets of opportunity provided by the Internet.

4.1 Low Risk

There is significant risk associated with an attempt to physically break into a house or business to steal money, equipment, or sensitive information. The likelihood of being caught in the act or leaving a plethora of DNA, fingerprints, shoeprints, hair and clothing particles, or security camera footage proving you were there is high. The effort and planning that are required to mitigate the risk of being caught or identified is correspondingly high. This level of preparation is not necessary for the criminal who uses a computer to attack the target's digital information and resources. Obscuring one's IP address and using other means to hide digital tracks is child's play for the amateur cracker. Specialized software to attack thousands of targets can be obtained for free through open-source means and run on Kali Linux, an operating system distribution specifically designed for network penetration [9]. In comparison to a physical crime, the relative anonymity of the attacker is high and the time and resource requirements for the attack are minimal.

4.2 Increasing Targets of Opportunity

Every year, the world population continues its exponential growth. As more and more children are born, the number of potential computer users increases accordingly. Criminals largely tend to attack targets of

opportunity. [4] state:

"For the usual predatory crime to occur, a likely offender must find a suitable target in the absence of a capable guardian. This means that crime can increase without more offenders if there are more targets, or if offenders can get to targets with no guardians present. This also means that community life can change to produce more crime opportunities without any increase in criminal motivation" [4].

Criminal acts, or attempts at criminal acts, involving the internet and digital connectivity will continue to increase as the target of opportunity increases. Internet connectivity has grown from 14.1% of the world's population in 2004 to 40.4% in 2014 [8]. Due to the increasing transition to digital records and transactions, as well as the sharing of personal information online, this target will continue to grow more and more enticing for those with the intent to blackmail, extort from, masquerade as, and steal from others.

5. Impact of Cybercrime on Organizations

Cybercrime is not an occurrence to be taken lightly. It may seem to be most devastating to the individual computer user due to the personal nature of the information compromised or funds stolen. However, organizations stand to lose much as well, and the damage done to them in the form of money, reputation, and time lost can be much more destructive in the long run due to the many people that are affected—employees and customers alike.

5.1 Financial Damage

The financial expense resulting from a successful network intrusion can be staggering. According to the [12], in the United States, "The average cost for each lost or stolen record containing sensitive and confidential information increased from $201 to $217" and "the total average cost paid by organizations increased from $5.9 million to $6.5 million" from 2013 to 2014 [12]. The financial loss to an organization is not just calculated by how much money was taken by the attackers. It includes an estimate of the business that was lost due to non-availability of online resources in the case of a denial-of-service attack, as well as the cost of recovering deleted information in the event of a malicious attack involving the destruction of data. Additionally, the company may need to hire outside specialists to conduct a more thorough recovery, or pay for over-time for IT employees during the recovery operation.

5.2 Reputational Damage

A manager once worked for would frequently define trust as a "reservoir of fulfilled expectations". According to this definition, whatever an organization does that fulfills the expectations of its customers builds their trust and adds to the reservoir. Whenever those expectations are unfulfilled, that trust reservoir is diminished. A data breach, such as the one for Target in 2013, which resulted in over 40 million credit and debit card records compromised as well as names, addresses, and phone numbers of over 70 million customers [15], is a huge drain on the trust of its customers. A loss of customer trust in a company leads to business lost for that company as they will be less likely to trust it with sensitive information required for business transactions. Additionally,

when employees lose trust in their employer, they are more likely to start looking for work elsewhere. This is likely to negatively impact their dedication to the company and result in less productivity, creating a downward spiral for business. Loss of employee trust leads to higher attrition and emigration to competitors, continuing the downward trend for the organization that failed in its security.

5.3 Time Lost to Recovery

The third area of damage to an organization following a successful cyber-attack is time. Time drain results from having to recreate deleted records, notify employees and customers of the organization who have been victimized, and find and fix loopholes and harden the network to prevent further exploitation. [6] wrote that Sony Pictures Entertainment took over eight days to recover from the cyber-attack it suffered in December of 2014 [6], stating that the company "shut down its internal computer network…to prevent the data-wiping software from causing further damage, forcing employees to use paper and pen"[6]. Network hardening and troubleshooting can be especially time-consuming for IT personnel and can take their focus off daily network operations, resulting in slower response time to help-desk requests and network maintenance. This creates a domino effect in which business efficiency falls even more due to the increased time it takes the rest of the organization to accomplish simple, daily operations requiring network resources.

6. Recommendations for Preventative Measures and Solutions to Vulnerabilities

Though the vulnerability of an organization to social engineering attacks will never be entirely removed, there are several preventative measures and solutions this vulnerability that can be taken. Because of the human element, simply implementing additional technical authorization mechanisms is not enough. Thorough training, frequent social engineering drills (such as bogus internal phishing attacks) and penetration tests, and an overall focus on organizational discipline are necessary.

6.1 Awareness Training

Enterprise Risk Management [3] claims "training your employees is the best possible investment you could make to combat the threat of social engineering. An employee with an awareness of social engineering techniques will be able to proactively identify the traps and pitfalls commonly used" [3]. It further states:

Employee training and awareness programs should be tailored to meet audiences of varying technical levels. The "human firewall" can be strengthened by making employees fully aware of the organization's policies and procedures. Targeted and focused programs are the most effective long-term tool against social engineering. [3]

6.2 Regular training

An organization needs to conduct regular and redundant training on the means and methods of social engineering as well as the likelihood of attack. This training must be tightly ensured for each new employee before they gain access to the computer network or a put into any position that requires contact with non-employees. New employees are an easy target as they will likely not be as familiar with the faces that make up

the organization as their experienced counterparts are.

6.3 Thorough training

This awareness training needs to address as many aspects of social engineering as possible. It is impossible to perfectly predict that an intruder would use pretexting or phishing and not shoulder surfing or piggybacking. Even obscure means of attack should be discussed. A lack of breadth in what techniques are covered can result in employees being falsely confident that they can spot and defeat a social engineering attack, leaving them wide open to less commonly used methods.

6.4 Relevant training

The training the organization conducts must be engaging, enjoyable, current, and relevant. It should not be so boring or ill-presented as to become a chore for the employees to have to sit through it. If the IT or management personnel are unable to come up with an enjoyable, engaging way to train the rest of the organization, outside subject matter experts should be brought in who specialize in conducting such training in an effective manner.

6.5 Frequent Social Engineering Drills and Penetration Tests

A way to bring home just how easy it is to become the victim of a social engineering attack is to conduct drills and unscheduled penetration tests on a regular basis. Many penetration testing companies provide this service as a part of their vulnerability assessment. Peter Kim describes an example of his penetration testing company conducting what he calls the “SMTP Attack”:

In the following example, we are targeting the fake site bank.com, who has a subsidiary in Russia. The fake bank owns ru.bank.com and has MX records to that FQDN. Also, company.com (another fake company), owns us.company.com and has MX records for that FQDN. In this fake example, we purchase both the doppelganger domains uscompany.com and rucompany.com. If anyone mistypes an email to either domain, we will be able to inject ourselves into the middle of this conversation. By a few simple python scripts, when we receive an email from john@us.company.com to bob@rubank.com (mistyped doppelganger for ru.bank.com), our script will take that email and create a new email to bob@ru.bank.com (the proper email address) and sourced from john@uscompany.com (the mistyped doppelganger that we own). That means any reply response to John from Bob will come back through us. Now we have a full “Man in the MailBox” configured and can either just passively listen or attack the victims based on the trust factor they have for each other. [9]

However, the IT and facilities teams responsible for physical security should collaborate to conduct regular in-house drills, to reinforce the importance of vigilance on the employee population. Results of these drills and tests should be publicized (in an appropriate forum) for all to learn from and to showcase everyone’s ongoing vulnerability.

6.6 Organizational Discipline

Organizations must create security policies that include specific, detailed steps to verifying the authenticity of a person interacting with the company. Additionally, policies and procedures must clearly and succinctly address all possible avenues of attack or areas where employee complacency creates gaping security holes. These policies should be published and posted in appropriately related areas such as at reception desks, by phones, and next to workstations, as well as in restrooms and breakrooms, and by watercoolers and coffee pots, where employees frequently go for downtime. Specific procedures should be simplified to a list for placement in areas where there is a high probability of attack, such as next to secretary telephones or at the reception desk.

Discipline must be a primary focus in the organization—policies must be taken seriously and followed. Management must enforce those policies and treat lapses in network security as seriously as they treat violations of physical security procedures. With the revolving door of employee turnover throughout the years, new employees who are uninformed and inexperienced will constantly join the organization. If there is an atmosphere of compliance with published policies and a commitment to safeguarding a secure environment, the risk that a new hire will remain ignorant or complacent toward security is significantly mitigated. Security issues should be a normal and common part of regular conversation in the workplace.

7. Conclusion

Social engineering will continue to threaten network security as long as we rely on people in the operation of organizations. As much as we may like to think that we can patch any tear, plug any hole, and close any loophole in the way that we protect ourselves and our data, this vulnerability cannot be completely removed. Every year, informed, experienced, and prepared employees leave a company for a variety of reasons and new hires take their place at the oar. These new employees lack the training and knowledge that their predecessors were given and will fall prey to old tricks, schemes, and cons that generations before them succumbed to unless they are intentionally prepared. The best we can do is to conduct regular, thorough, and relevant awareness training, frequent drills and realistic tests, and maintain a steady focus on the overall discipline of the organization. In this way, we will harden that component of the network that is the softest by nature—the human being.

References

[1] Braiker, H. B. (2004). Who's pulling your strings?: How to break the cycle of manipulation and regain control of your life. New York, NY: McGraw-Hill.

[2] Curry, S. J. J. (2013). Instant-messaging security. In J. Vacca (Ed.), Computer and information security handbook (2nd ed., p. 727). Boston, MA: Morgan Kaufmann.

[3] Enterprise Risk Management. (2009, November). Social engineering: People hacking. Retrieved from http://www.emrisk.com/sites/default/files/newsletters/ERMNewsletter_november_2009.pdf

[4] Felson, M., & Clarke, R. V. (1998). Opportunity makes the thief: Practical theory for crime prevention (Police Research Series Paper 98). Retrieved from

http://webarchive.nationalarchives.gov.uk/20110218135832/rds.homeoffice.gov.uk/rds/prgpdfs/fprs98.pdf

[5] Granger, S. (2010, November 3). Social engineering fundamentals, part 1: Hacker tactics. Retrieved from http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics

[6] Grover, R., Hosenball, M., & Finkle, J. (2014, December 3). Sony Pictures struggles to recover eight days after cyber attack. Retrieved from http://www.reuters.com/article/2014/12/03/us-sony-cybersecurity-investigation-idUSKCN0JG27B20141203

[7] References marked with an asterisk indicate studies included in the meta-analysis.

[8] *Internet Live Stats. (2014, July 1). Internet users in the world. Retrieved from http://www.internetlivestats.com/internet-users/

[9] Kim, P. (2014). The hacker playbook: Practical guide to penetration testing. North Charleston, SC: Secure Planet.

[10] Mitnick, K. D., & Simon, W. L. (2011). Ghost in the wires: My adventures as the world's most wanted hacker. New York, NY: Back Bay Books.

[11] Pagliery, J. (2014, May 28). Half of American adults hacked this year. Retrieved from http://money.cnn.com/2014/05/28/technology/security/hack-data-breach/

[12] *Ponemon Institute. (2015, May). 2015 Cost of data breach study: United States. Retrieved from IBM website: http://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03055usen/SEW03055USEN.PDF

[13] Simon, G. K. (2010). In sheep's clothing: Understanding and dealing with manipulative people (2nd ed.). Little Rock, AR: Parkurst Brothers.

[14] *Statista. (2015, August). Number of compromised data records in selected data breaches as of August 2015. Retrieved from http://www.statista.com/statistics/290525/cyber-crime-biggest-online-data-breaches-worldwide/

[15] Yang, J. L., & Jayakumar, A. (2014, January 10). Target says up to 70 million more customers were hit by December data breach. Retrieved from http://www.washingtonpost.com/business/economy/target-says-70-million-customers-were-hit-by-dec-data-breach-more-than-first-reported/2014/01/10/0ada1026-79fe-11e3-8963-b4b654bcc9b2_story.html

Works Consulted

[16] Al-Johani, A. A., & Al-Msloum, A. S. (2013, November). Social engineering risks in the contemporary reality and methods of fighting these risks. International Journal of Academic Research, 5(6), 265-272. http://dx.doi.org/10.7813/2075-4124.2013/5-6/A.33

[17] Allen, M. (2006, June). Social engineering: A means to violate a computer system. Retrieved from https://www.sans.org/reading-room/whitepapers/engineering/social-engineering-means-violate-computer-system-529

[18] Bavisi, S. (2013). Penetration testing. In J. Vacca (Ed.), Computer and information security handbook (2nd ed., p. 535). Boston, MA: Morgan Kaufmann.

[19] Bidgoli, H (Ed.). (2006). Handbook of information security: Threats, vulnerabilities, prevention, and management. Hoboken, NJ: John Wiley & Sons.

[20] CBS. (2015, March 3). These cybercrime statistics will make you think twice about your password: Where's the CSI cyber team when you need them? Retrieved from http://www.cbs.com/shows/csi-cyber/news/1003888/these-cybercrime-statistics-will-make-you-think-twice-about-your-password-where-s-the-csi-cyber-team-when-you-need-them-/

[21] Chen, T., & Walsh, P. (2013). Guarding against network intrusions. In J. Vacca (Ed.), Computer and information security handbook (2nd ed., p. 83). Boston, MA: Morgan Kaufmann.

[22] Crank, C. (2014, June 30). Social engineering: How it's used to gain cyber information. Retrieved from http://www.scmagazine.com/social-engineering-how-its-used-to-gain-cyber-information/article/358339/

[23] Criddle, L. (2015). What is social engineering? Retrieved from http://www.webroot.com/us/en/home/resources/tips/online-shopping-banking/secure-what-is-social-engineering

[24] DiBello, A. (2014, December 29). Social engineering will ramp up in 2015. Retrieved from http://www.scmagazine.com/social-engineering-will-ramp-up-in-2015/article/389169/

[25] El Emary, I., Shalhoub, M., Arif, M., Alsereihy, H., Shalhoub, L., & Al-Sahhaf, N. (2013, January). Social engineering and its effective role in securing and defending the knowledge community. International Journal of Academic Research, 5(1), 95-100. http://dx.doi.org/10.7813/2075-4124.2013/5-1/A.15

[26] Goodrich, M., & Tamassia, R. (2011). Introduction to computer security. Boston, MA: Pearson.

[27] Greabu-Serban, V., & Serban, O. (2014). Social engineering a general approach. Informatica Economica, 18(2), 5-14. http://dx.doi.org/10.12948/issn14531305/18.2.2014.01

[28] Hadnagy, C. (2010). Social engineering: The art of human hacking. Indianapolis, IN: Wiley

[29] Hadnagy, C. (2014). Unmasking the social engineer: The human element of security. Indianapolis, IN: John Wiley & Sons.

[30] Harley, D. (1998). Re-floating the Titanic: Dealing with social engineering attacks. In EICAR 98 Conference Proceedings [Compact disk]. EICAR. Retrieved from http://cluestick.info/hoax/harley_eicar98.htm

[31] Harman, P. (2015, May 13). Businesses beware: Social engineering fraud could cost you millions. Claims Magazine, 63(6), 12-13. Retrieved from http://www.propertycasualty360.com/2015/05/13/businesses-beware-social-engineering-fraud-could-c

[32] Harman, P. (2015, August 7). Social engineering scams: How hackers are stealing from your clients. Retrieved from http://www.propertycasualty360.com/2015/08/07/social-engineering-scams-how-hackers-are-stealing

[33] Harman, P. (2015, October 2). Cyber crime: The gift that keeps on giving. Retrieved from http://www.propertycasualty360.com/2015/10/02/cyber-crime-the-gift-that-keeps-on-giving

[34] Honan, B. (2015, August 6). Ubiquiti Networks victim of $39 million social engineering attack. Retrieved from http://www.csoonline.com/article/2961066/supply-chain-security/ubiquiti-networks-victim-of-39-million-social-engineering-attack.html

[35] *IBM Security. (2015). IBM 2015 cyber security intelligence index. Retrieved from IBM website: http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEW03073USEN&attachment=SEW03073USEN.PDF

[36] Lascano, S. (2014, September 4). Malware bypasses Chrome extension security feature. Retrieved from http://blog.trendmicro.com/trendlabs-security-intelligence/malware-bypasses-chrome-extension-security-feature/

[37] Lieu, C. (2002). Social engineering - attacking the weakest link. Retrieved from https://www.giac.org/paper/gsec/2082/social-engineering-attacking-weakest-link/103563

[38] Mitnick, K. D., & Simon, W. L. (2003). The art of deception: Controlling the human element of security. Indianapolis, IN: Wiley.

[39] Patil, H., Wing, D., & Chen, T. (2013). VoIP security. In J. Vacca (Ed.), Computer and information security handbook (2nd ed., pp. 877-878). Boston, MA: Morgan Kaufmann.

[40] Peters, S. (2015, March 17). The 7 best social engineering attacks ever. Retrieved from http://www.darkreading.com/the-7-best-social-engineering-attacks-ever/d/d-id/1319411

[41] Social-Engineer.Org. (2014, April 28). The social engineering infographic. Retrieved from http://www.social-engineer.org/social-engineering/social-engineering-infographic/

[42] Swanson, C., Chamelin, N., Territo, L., & Taylor, R. (2011). Criminal investigation (11th ed.). New York, NY: McGraw-Hill.

[43] Valacich, J., & Schneider, C. (2014). Information systems today: Managing in the digital world (6th ed.). Boston, MA: Pearson.

[44] Walker, D. (2014, May 29). Iranian spies bait U.S. officials in years-long social engineering scheme. Retrieved from http://www.scmagazine.com/iranian-spies-bait-us-officials-in-years-long-social-engineering-scheme/article/349079/

[45] Walker, D. (2014, June 11). Clandestine Fox attack op uses social engineering to woo new victims. Retrieved from http://www.scmagazine.com/clandestine-fox-attack-op-uses-social-engineering-to-woo-new-victims/article/355318/

[46] Webopedia. (n.d.). Social engineering. Retrieved from

http://www.webopedia.com/TERM/S/social_engineering.html

[47] Weise, E. (2014, September 24). 43% of companies had a data breach in the past year. Retrieved from http://www.usatoday.com/story/tech/2014/09/24/data-breach-companies-60/16106197/

Cybercrime, which has also been called â€œcomputer crimeâ€, â€œdigital crimeâ€, â€œInternet crimeâ€, and â€œhigh-tech crimeâ€, is commonly understood to include a broad range of criminal activities that use computers, digital devices, and the Internet. Despite almost forty years of incidents, cybercrime still does not have a universally accepted definition in literature. Most authors classify cybercrimes based on the role of technology and criminal modus operandi. We have adapted a general framework and set of definitions11 12 13 to set the context for the current work and will consider and explain cyberc... Table 1. Cybercrime, Data Breaches, and Data Security Table 2. National Security, Cyber Espionage, and Cyberwar Table 3. Cloud Computing, "The Internet of Things," Smart Cities, and FedRAMP. Summary. As online attacks grow in volume and sophistication, the United States is expanding its cybersecurity efforts.Â credit bureaus, and the Internal Revenue Service. (IRS) among others. Health and Human Services (HHS). Continuously Updated. As required by Section 13402(e)(4) of the HITECH Act, P.L. 111-5 HHS must post a list of breaches of unsecured protected health information affecting 500 or more individuals. Cybercrime is one of the fastest-growing criminal activities on the planet. Cybercrime is defined as the use of any computer network for crime and the high-tech criminals of the digital age have not been slow to spot the opportunities. Cybercrime covers a huge range of illegal activity including financial scams, computer hacking, downloading pornographic images from the Internet, virus attacks, stalking by e-mail and creating websites that promote racial hatred. The term hacking was originally used to describe the activities of computer enthusiasts who pit their skills against the IT systems o The basic 'good' human nature characteristics make people vulnerable to the techniques used by social engineers, as it activates various psychological vulnerabilities, which could be used to manipulate the individual to disclose the requested information [50,51,52,53] The exploitation of the human factor has extensive use in advanced persistent threats (APTs).Â Online social networks (OSNs) are ubiquitous attracting millions of users all over the world. Being a popular communication media OSNs are exploited in a variety of cyber attacks. In this article, we discuss the Chameleon attack technique, a new type of OSN-based trickery where malicious posts and profiles change the way they are displayed to OSN users to conceal themselves before the attack or avoid detection. Human weaknesses are generally exploited. The damage dealt is largely psychological and intangible, making legal action against the variants more difficult. These are the crimes which have existed for centuries in the offline world.Â It is not only the US and the European Union who are introducing new measures against cybercrime. ON 31 May 2017 China announced that its new cybersecurity law takes effect on this date.[82].