Review Article

International Journal of Advanced Computer Research, Vol 6(23)
ISSN (Print): 2249-7277   ISSN (Online): 2277-7970
http://dx.doi.org/10.19101/IJACR.2016.623006

Cybersecurity:risks, vulnerabilities and countermeasures to prevent social engineering attacks

Nabie Y. Conteh[1*] and Paul J. Schmick[2]
Assistant Professor, Department of Computer Information Systems, College of Business & Public Administration, Southern University, New Orleans, Louisiana, USA[1]
Department of Cyber Security and Information Assurance, Graduate School of MGT and Technology, University of Maryland University College, Adelphi, Maryland, USA[2]

Received: 21-December-2015; Revised: 07-February-2016; Accepted: 10-February-2016

Abstract

The broad objective of this study is to evaluate the vulnerabilities of an organization's information technology infrastructure, which include hardware and software systems, transmission media, local area networks, wide area networks, enterprise networks, intranets, and its use of the internet to cyber intrusions. To achieve this objective, the paper attempts to explain the importance and the role of social engineering in network intrusions and cyber-theft. It also discusses in vivid detail, the reasons for the rapid expansion of cybercrime. The paper also includes a complete description and definition of social engineering, the role it plays in network intrusion and cyber identity theft, a discussion of the reasons for the rise in cybercrime and their impact on organizations. In closing the authors recommend some preventive measures and possible solutions to the threats and vulnerabilities of social engineering. The paper concludes that while technology has a role to play in reducing the impact of social engineering attacks, the vulnerability resides with human behaviour, human impulses and psychological predispositions. While literature supports the dangers of psychological susceptibilities in social engineering attacks investment in organizational education campaigns offer optimism that social engineering attacks can be reduced.

Keywords

Cyber security, Cyber theft, Social engineering, Cybercrime, Phishing, Network intrusions.

1.Introduction

Social engineering, also known as human hacking, is the art of tricking employees and consumers into disclosing their credentials and then using them to gain access to networks or accounts. It is a hacker's tricky use of deception or manipulation of people's tendency to trust, be corporative, or simply follow their desire to explore and be curious. Sophisticated IT security systems cannot protect systems from hackers or defend against what seems to be authorized access. People are easily hacked, making them and their social media posts high-risk attack targets. It is often easy to get computer users to infect their corporate network or mobiles by luring them to spoof websites and or tricking them into clicking on harmful links and or downloading and installing malicious applications and or backdoor's.

In a 2013 study conducted by TNS Global for Halon an email security service, 30 percent of the surveyed populace comprised of 1,000 adults in the U.S. disclosed that they would open an e-mail even if they were aware it contained a virus or was suspicious [1]. Even with robust campaigns conveying the dangers of opening suspicious e-mails a large majority of email users remain vulnerable to social engineering attacks [2]. To confront the challenges posed from social engineering attacks, recommendations deriving from research offer options to reduce the probability of success of a social engineering attack.

With cyber security incidents growing exponentially in terms of frequency and damage to an organizations reputation in their respective marketplace, users and organizations have not adequately deployed defenses to discourage would-be attacker's intent to strike. The terms information and network security continue to dominate U.S. headlines with a large-scale cyber-attack surpassing the probability of a physical terrorist attack on U.S. soil. In fact, in a 2013

[*] Author for correspondence

interview of FBI Director James Comey, the Director testified before a Senate Homeland Security Committee that cyber-attacks have surpassed terrorism as a major domestic threat, with the threat continuing to rise [3].

In this paper social engineering is defined along with the types of social engineering attacks. In addition, this research will identify why cyber theft continues to advance at an alarming rate. Furthermore, psychological variables that contribute to vulnerabilities will be discussed. And finally, studies will be presented that identify key considerations regarding social engineering, testing and training, and point to how users can be coached to prevent attacks which offers a promising methodology to reduce system and user's risk.

2.What is social engineering?

Engebretson (2011) [4] defines social engineering as “one of the simplest methods to gather information about a target through the process of exploiting human weakness that is inherit to every organization.” The foundation of an attack is to persuade the forfeiture of information that is confidential then exploit an individual or an organization. In essence, an attacker engages social engineering as a tactic to use human insiders and information to circumvent computer security solutions through deceit.

Regarding the human vulnerability of social engineering [5] note that while social engineering is identified as a low-tech attack; the attack aims at manipulating victims to divulge confidential information and is successful in its attempt due to exploiting personality vulnerabilities. Social engineering as a tactic deploys techniques to gain access to private and confidential information by exploiting flaws in human logic know as cognitive biases [5]. While security technology measures aim at improving information system security, human factors represent a weak-link which is exploited during a social engineering attack. Bisson (2015) [6] notes that social engineering is “a term that encompasses a broad spectrum of malicious activity” and identifies five of the most common types of social engineering attacks to target victims which include:

Phishing: Phishing scams attempt to obtain personal information such as names, addresses and other personal identifiable information (PII) such as social security numbers. Phishing scams may embed links to redirect users to suspicious websites that appear legitimate. These types of scams create a sense of urgency to manipulate users to act in a manner that challenges good judgment.

Pretexting: This type of social engineering attack is driven by a fabrication scenario attempting to confirm and steal personal information from a target. Advanced attacks attempt to exploit a weakness of an organization or company. This method requires the attacker to build a credible story that leaves little room to question doubt by a target. The strategy is to use fear and urgency while building a sense of trust with a victim to confirm or obtain sought information.

Baiting: Baiting is similar to a phishing attack, but lures a victim through enticement strategies. Hackers use the lure of promised goods if a user surrenders log-in credentials to a specific site. Baiting schemes are not limited to, digital on-line schemes and can also be launched through the use of physical media.

Quid pro quo: Similar to Baiting, but this type of threat is presented as a technical service in exchange for information. A common threat is for an attacker to impersonate an information technology representative and offer assistance to a victim who may be experiencing technical challenges. The attacker aims to launch malware on a user’s system.

Tailgating: This type of attack uses tailgating and piggybacking to gain access to restricted areas. This attack exposes those who have an ability to grant or gain access to a restricted area by an attacker who may impersonate delivery personnel or others who may require temporary access.

3.Social engineering and its role in cyber-theft

Information Security is defined as “protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction” according to U.S. law [7]. And while so much attention in terms of resources and training to overcome information security breaches have been deployed, Nakashima and Peterson (2014) [8] note the center for Strategic and International Studies identifies the annual cost of cybercrime and economic espionage to cost to global economy more than $445 billion annually–or almost one percent of total global income [9].

Hackers are getting increasingly sophisticated and adept at their social engineering attacks. They are able to piece together disparate data from various sources and namely, social media, corporate blogs, and data and to painstakingly pull crucial and key data from well-meaning employees, which these cyber-criminals use to attack networks and steal invaluable data and even hold corporations hostage and in some cases damage the object of their targets.
Regarding the rise of cybercrime and theft, Grimes (2014) [10] identifies key indicators as to the rise and cause of cybercrime which financially impacts both individuals and organizations. One reason for cyber theft appeal is the benefit of theft by ambiguity. Internet crimes are committed by thousands of cyber criminals world-wide, but few are prosecuted and jailed. In addition, cyber criminals do not have to be intelligent to be successful in digital theft, but are willing to take risks because of the benefits of distance from a victim while taking little risk and little exposure.

Many cyber thefts take place globally and law enforcement agencies are limited to the jurisdictional boundaries to pursue cyber criminals. The pursuit also includes working with other law enforcement agencies outside of domestic jurisdictions. While this is less complex domestically, getting international support to pursue international theft remains a challenge for U.S. Law enforcement. In essence, most international governments do not cooperate with each other [11].

Evidence plays another factor and a lack of successful convictions is due to a lack of evidence that can be delivered in court to prosecute cyber criminals. Two primary variables relate to evidence fulfilment, such as obtaining evidence that is credible to hold individuals accountable. Second, few organizations have the legal expertise to prepare legal evidence in cybercrime cases which takes planning, commitment and resources. These challenges lower the probability that a criminal even if caught will be prosecuted and jailed.

To overcome crime in the cyber domain, a lack of resources is perhaps the leading contributor to its exponential growth. Few organizations have the dedicated resources to pursue internet crimes and criminals. The challenge of pursuing cyber theft is costly and without a potential return-on-investment (ROI) dedicated resources are difficult to justify.

While the cost of cyber victimization is nearly a half trillion dollars, it has not hurt global economies and may even be in the realm of appearing as a cost of doing business. For meaningful change to occur, once cybercrime hurts individuals and organizations to an unbearable point, the reality or managing risk and loss have been built into the fabric of organizations, and individual victimization from small-scale occurrences have become noise that is expected.

4.Psychological variables and contribution to cybercrimes

Social engineering attacks challenge information security professionals because no technical countermeasures to-date can eliminate the human vulnerability [5]. Identifying the cause of human error and successful social engineering attacks Luo, et al. (2011)[5] argues the social psychology influences of “alternative routes to persuasion, attitudes and beliefs that affect human interactions, and techniques for persuasion influence” expose the psychological vulnerabilities that enable a successful social engineering attack.

To seek foundations of the interest to open potentially damaging e-mails, Ragan (2013) [1] notes the diversity of intent to engage in such behaviour is specific among genders with women enticed to open malicious e-mails appearing from social networks, while men fall prey to e-mails communicating power, money and sex. Because social engineering attacks, tap into human psychological impulses reducing engagement remains a challenge because occurrences aim at human psychological vulnerabilities [12].

Further evaluating the social psychological influences, alternate routes to persuasion contribute to successful social engineering attacks through influencing a victim’s emotions towards fear or excitement which may alter a responsible action. Regarding attitudes and beliefs, this refers to the differences concerning the beliefs between the victim and his/her social engineering attackers. And lastly, influencing techniques relies on peripheral paths to persuasion that influence behaviour and action [5].

Because of the emotional exposure and triggered a response initiated by social engineering attacks, without awareness of the vulnerabilities revealed by artful exposure of human susceptibility to engage in the process, denying an attackers ploy is a challenge.

However, studies demonstrate awareness through corporate education campaigns may provide a virtual barrier to reduce the success rate of social engineering attacks. In totality, the chief strategy may reside in awareness in the manipulation tactics to obtain valuable and confidential information to prevent social engineering attackers’ from acquiring information to exploit a user or organization.

5.Social engineering techniques–human and technical

Luo et al. (2011) [5] identifies several human or technical means that social engineering attackers can deploy from phishing to dumpster diving as tactics to gain visibility or obtain confidential information. For aggressive and successful attackers a synergy of human and technical strategy may be deployed to obtain ample information on an individual or to gain access to an organization. Regarding the steps of gathering information through execution of a social engineering attack Luo et al. (2011) [5] identify the steps in the attack process.

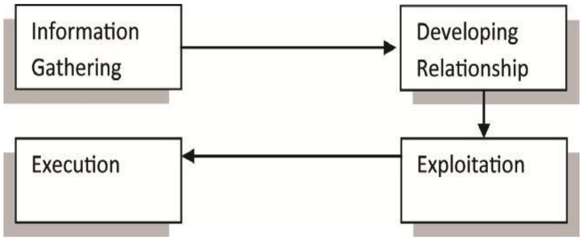


Figure 1 Four steps of social engineering [5]

Figure 1 above graphically explains the stepwise approaches in the execution of social engineering attacks. The process begins with the first phase of studying and gathering information, then a relationship is established. In the exploitation phase, access into the system is gained and in the final phase, the attacked is implemented.

Social engineering attacks can be categorized in either human or technology deployments. Direct human engagement stems from an attacker who has obtained personal information about a victim and develops a relationship with the user. Because the attacker deploys a strategy of a known or trusted party, the victim becomes susceptible and exploited, and relinquishes sensitive or personal company information; therefore contributing to the pieces of the puzzle the attacker can use to his/her advantage. Technical attacks are more unambiguous and deployed through a host of options such as; software programs, email attachments, pop-up windows and websites [5]. Perhaps the most successful technical ploy to draw a user into divulging account usernames and passwords by prompting victims to input user and password information in pop-up windows. Websites and pop-up windows can appear as a site frequently visited by a user, however, the script-embedded pop-up window manipulates the user to enter a username and password which delivers the information to the attacker.

6.Preventive measures against social engineering

It is evident that regardless of how technologically secure a network seems the human element will always be a vulnerability. The success rate and the number of cybercrimes are steadily on the rise due to the level of anonymity social engineering offers malicious actors. Businesses have to remain cognizant of the various threat actors and their plethora of attacks so they are able to respond accordingly. There are technical and non-technical safeguards that can be implemented to lower the risk associated with social engineering to a tolerable level. Companies are adding multiple layers to their security schemes so that if the mechanism in the outer layer fails, a mechanism in at least one inner layer can help prevent a threat from turning into a disaster (Risk Mitigation). This concept is known as multi-layer defense or defense in depth. A good Defense in Depth structure includes a mixture of the following precautionary measures:

Security Policy: A well written policy should include technical and nontechnical approaches that are downward driven by executive management. Every organization should integrate security into their operational objectives.

Education and Training: Employees ought to be required to attend initial training during orientation and recurring refresher trainings. This builds awareness by exposing users to commonly employed tactics and behaviors targeted by a social engineer.

Network Guidance: The organization have to safeguard the network by whitelisting authorized websites, using Network address translation (NAT), and disabling unused applications and ports. Network users have to maintain complex passwords that are changed every 60 days.

Audits and Compliance: Organizations have to actively verify that their security policy is being adhered to. Some detective controls include reviewing network logs, re-validating employees' permissions, and checking desktop configurations at least bi-monthly.

Technical Procedures: The network should have multiple layers of defence to protect data and core infrastructure. Software like Intrusion Prevention Systems (IPS), Intrusion Detection Systems (IDS) and firewalls should be installed on every device. Demilitarized Zones (DMZ), web filters and Virtual Private Network (VPN) should be installed on all external facing services.

Physical Guidance: There is a range of options that can be implemented to protect physical assets. Using a combination of security guards, mantraps and security cameras to deter intruders from entering the premises is beneficial. In places where physical hardware is located businesses should employ multifactor authentication, biometrics or access control list before access is granted.

To overcome the challenges of social engineering attacks Luo et al. (2011) [5] identify the necessity of a multidimensional approach to overcome threats through a holistic approach of addressing organizational policies, procedures, standards, employee training and awareness programs, and incident response. While all areas to combat this threat are critical, without employee training expensive infrastructure and network security investment means little considering only seven percent of U.S. organizations deploy training programs and materials in phishing education [13].

Evaluating variables of cause and identifying those who are susceptible in an organization Chitery, Singh, Bag, & Singh (2012) [14] identify the drivers, targets and motivation behind social engineering attacks. The 2012 study attempted to demonstrate an analytical approach towards social engineering attacks and identify attacker trends. The study, which surveyed an undisclosed amount of IT professionals, sheds light on potential training measures for organizations that are eager to deploy information security awareness programs to reduce the risk of employee proneness to a social engineering attack.

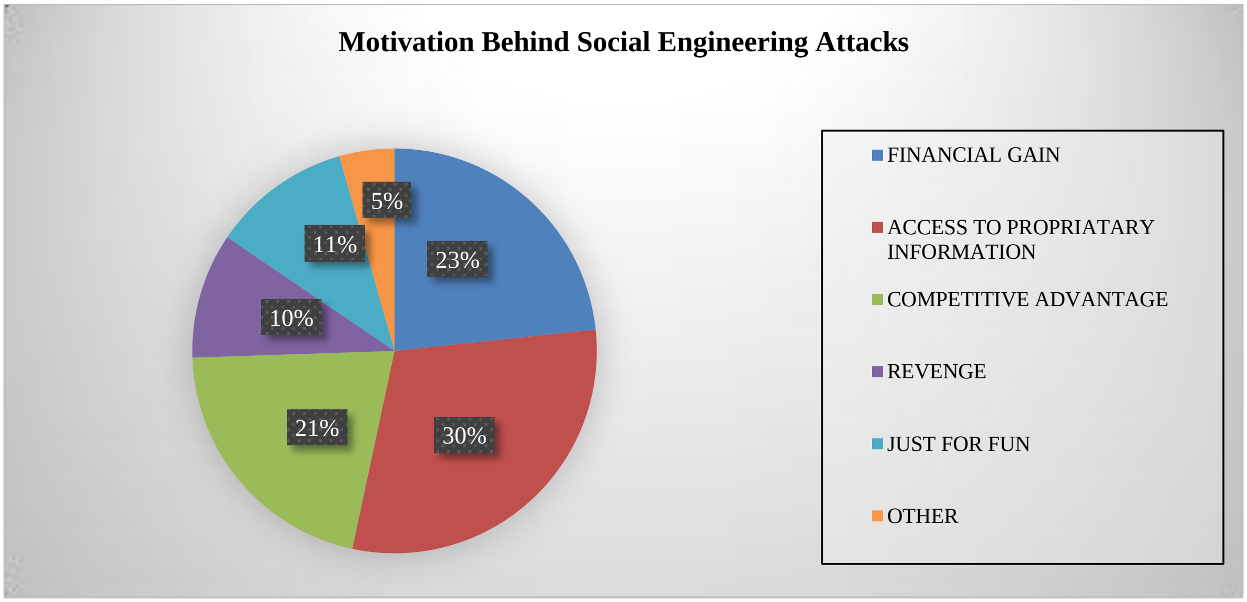


Figure 2 Questionnaire results regarding the motivation behind social engineering attacks

According to a study conducted by Chitery, Singh, Bag, & Singh (2012) [14] as introduced in the preceding paragraph above, *Figure 2* depicts the motivating factors behind social engineering attacks. It is evident that the access motivated by the need to gain proprietary information ranks the highest in terms of the volume which is 30%. Financial gain ranks second, followed by the need for competitive advantage, then by "just for fun", revenge and last and least by unnamed others. *Figure 3* depicts the results from the same study as above obtained on entities that are vulnerable to social engineering attacks. The most vulnerable group is the new employees (41%), followed by clients and customers (23%), then by IT professionals (17%), by Partners and Contractors (12%) and lastly followed by others.

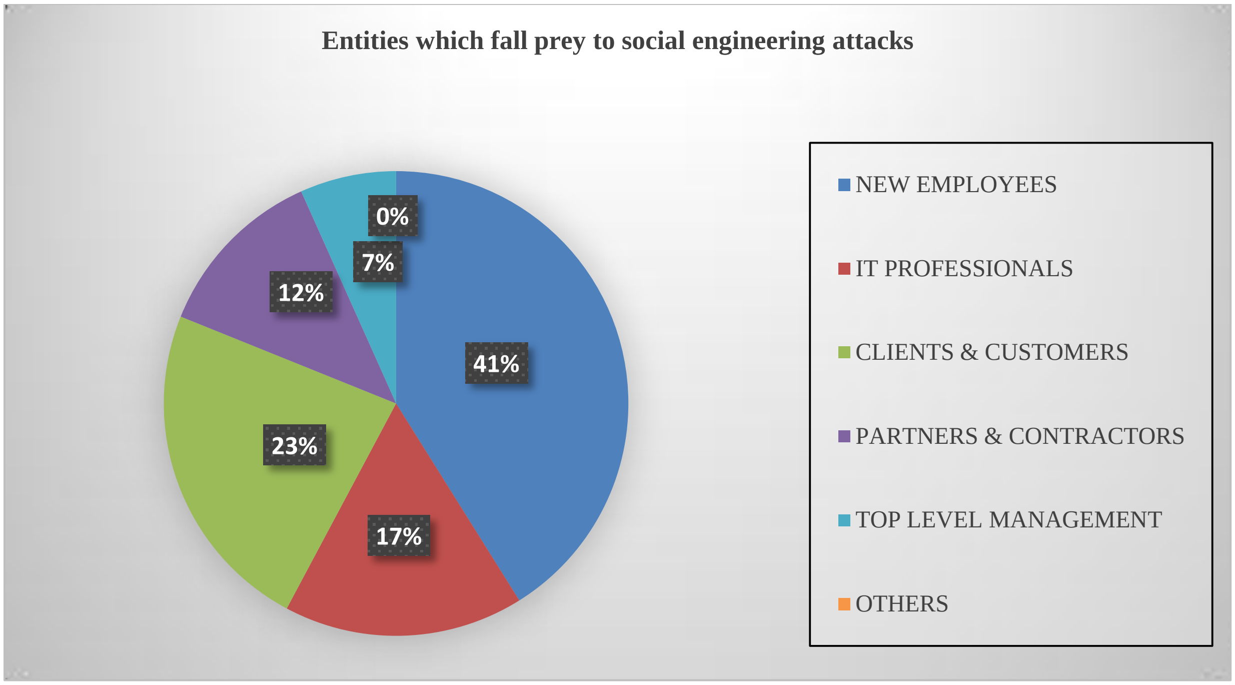


Figure 3 Questionnaire results regarding entities which present risk of falling prey to a social engineering attack

In another study by Bowen, Devarajan & Stolfo (2011)[15] this Columbia University study measured enterprise susceptibility to phishing attacks which is a technical path and deployment mechanism to instigate a social engineering attack. The 2011 study's primary focus conducted by Columbia University was on reinforced training and the impact to prevent social engineering attacks. As the results shown in *Table 1 and 2* below, the study tested user vulnerabilities using decoy e-mails to lure users to supply information or access phony e-mails so data could be gathered and utilized for training purposes to prevent future attacks.

Table 1 The number of responses for each round for the first experiment to measure the user response to phony phish

Decoy Type	**1st Round**	**2nd Round**	**3rd Round**	**4th Round**
Email with internal URLs	52	2	0	NA
Email with external URLs	177	15	1	0
Forms to obtain credentials	39/20	4/1	0	NA
Beacon Documents	45	0	NA	NA

Table 2 The number of responses for each round of the second experiment to measure the user response to phony phish

Decoy Type	**1st Round**	**2nd Round**	**3rd Round**	**4th Round**
Email with internal URLs	69	7	1	0
Email with external URLs	176	10	3	0
Forms to obtain credentials	69/50	10/9	0	NA
Beacon Documents	71	2	0	NA

The Bowen, et al. (2011) [15] study was conducted by deploying two rounds of experiments. Users were probed repeatedly, then educated each time to understand how the luring techniques occurred until victims stopped falling prey to attacks. The data ultimately support that both repetitious probes followed by education offers value and a return on investment (ROI) to limit successful probes of users regardless of psychological predispositions or gender. Evaluating the data from both rounds of the Columbia University experiment confirms users can be coached to deploy caution before opening suspicious e-mail messages.

As the data supports, by reaffirming threats through repetitive communication, although slower learners had the highest probability that they would fall-prey to social engineering attacks, users were still able to be coached to disengage in the luring process of social engineering attacks.

7.Limitations of the study

Luo et al. (2011) [5] recognizes key considerations that can be learned from social engineering penetration testing and education. Most importantly, the 2011 Columbia University study noted in this research paper identifies that education followed by additional social engineering, testing leads to a dramatic reduction in social engineering attack success, therefore reducing information system and network vulnerability. However, the 2011 Columbia University study offers no consideration to how frequently testing and training may be required to maintain the same results. In essence, the limitations of the Columbia University study prevents drawing an absolute conclusion that the same results should be expected if further testing was conducted. This leaves consideration to the deployment of recurrent training models after periods of time to determine if similar results can be produced by users after one phase of testing to determine if training efforts are lasting.

8.Conclusions

To overcome cyber security incidents involving social engineering attacks, research supports the most effective defence is an educated computer user. To consider is those most vulnerable which are identified in this research as new employees within an organization, as specifically shown in *Figure 3* above, with the attacker seeking personal identifiable information (PII) from those engaged. Further supported in this research are the psychological variables that contribute to user vulnerability. This paper concludes that while technology has a role to play in reducing the impact of social engineering attacks, the vulnerability resides with human behaviour, human impulses and psychological predispositions that can be influenced through education. Ultimately, investment in organizational education campaigns offer optimism that social engineering attacks can be reduced, but an absolute solution to overcome such cyber security threats has yet to be put-forward.

Acknowledgment

None.

Conflicts of interest

The authors have no conflicts of interest to declare.

References

[1] Ragan S, W Staff. Social engineering: study finds Americans willingly open malicious emails.http://www.csoonline.com/article/2133877/social-engineering/social-engineering--study-finds-americans-willingly-open-malicious-emails.html. Accessed 28 August 2013.

[2] Maan PS, Sharma M. Social engineering: a partial technical attack. International Journal of Computer Science Issues. 2012; 9(2):557-9.

[3] Anonymous. FBI: Cyber-attacks surpassing terrorism as major domestic threat. https://www.rt.com/usa/fbi-cyber-attack-threat-739/. Accessed 25 November 2013.

[4] Engebretson P. The basics of hacking and penetration testing: ethical hacking and penetration testing made easy. Elsevier; 2011.

[5] Luo X, Brody R, Seazzu A, Burd S. Social engineering: the neglected human factor for information security management. Information Resources Management Journal. 2011; 24(3):1-8.

[6] Bisson D. 5 Social engineering attacks to watch out for. The state of security. http://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/. Accessed 23 March 2015.

[7] Andress J. The basics of information security: understanding the fundamentals of InfoSec in theory and practice. Elsevier; 2011.

[8] Nakashima E, Peterson A. Report: cybercrime and espionage costs $445 billion annually. The Washington Post. https://www.washingtonpost.com/world/national-security/report-cybercrime-and-espionage-costs-445-billion-annually/2014/06/08/8995291c-ecce-11e3-9f5c-9075d5508f0a_story.html . Accessed 9 June 2014.

[9] Strohm C. Cyber theft, already a $445 billion business, to grow bigger. http://www.insurancejournal.com/news/national/2014/06/09/331333.htm. Accessed 9 June 2014.

[10] Grimes RA. 5 reasons internet crime is worse than ever. Info World. http://www.infoworld.com/article/2608631/security/5-reasons-internet-crime-is-worse-than-ever.html?page=2. Accessed 23 March 2015.

[11] Taylor RW, Fritsch EJ, Liederbach J. Digital crime and digital terrorism. Prentice Hall Press; 2014.

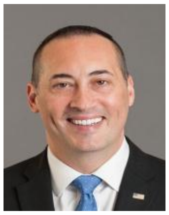
[12] Vacca JR. Computer and information security handbook. Newnes; 2012.

[13] Diana A. Social engineering targets weakest security link: employees. http://www.enterprisetech.com/2015/05/19/social-engineering-targets-weakest-security-link-employees/ Accessed 19 May 2015.

[14] Chitrey A, Singh D, Singh V. A comprehensive study of social engineering based attacks in India to develop a conceptual model. International Journal of Information and Network Security. 2012; 1(2):45-53.

[15] Bowen BM, Devarajan R, Stolfo S. Measuring the human factor of cyber security. In international conference on technologies for homeland security (HST) 2011(pp. 230-5). IEEE.

Dr. Nabie Y. Conteh is a Computer Information Systems Professor at Southern University at New Orleans (SUNO). He holds a BS in information systems from the Institute for Information and Communication Technology, in the Netherlands; an MBA in information systems management from Ferris State University; and an MS and Ph.D. in information systems from the University of Maryland, Baltimore County. His areas of teaching and research interest include decision support systems, systems modeling and simulation; artificial intelligence/expert systems; systems analysis and design; and knowledge management and organizational learning. Dr. Conteh possesses many technical skills and the ability to speak English, Dutch, Russian and German. Dr. Conteh has made many presentations at national and international conferences and has been published in refereed journals and proceedings. He has worked as Assistant Professor at Shenandoah University and is currently an Adjunct Associate Professor of Cyberspace and Cyber Security at the Graduate School of the University of Maryland University College and Professor of Database Management Systems and Global Information Technology at Florida Tech. During the tenure of his Ph.D. program, he worked as Research Assistant at the University of Maryland Baltimore County. He did consulting for Datastream at College Park in Maryland, a company whose primary activity is data conversion. He has also worked for Getronics Transaction Services and EuroShell International, ABN AMRO Bank at Amsterdam, in the Netherlands.
Email: nconteh@suno.edu



Paul J. Schmick is a Speaker, Professor and Vice President of Security Technology for Alliance Security Services headquartered in New York. Paul is a seasoned professional in the disciplines of security convergence and information technology, cybersecurity, physical security, risk-based security and security technologies. Paul previously held the position of Director of Corporate Security Programs at FJC Security Services where he directed the company's corporate security programs, managed FJC's Office of Information Technology (OIT), and was the Managing Director of FJC Technology Solutions where he directed the organizations security technology service division. Paul also served eight years with the U.S. Department of Homeland Security (DHS) - Transportation Security Administration (TSA) and in his last role with the department was responsible for the implementation of aviation security policy, managed security technology equipment deployments, and supervised training programs and personnel to enhance the agency's formidable defense against improvised explosive device (IED) threats targeting U.S. aviation assets and infrastructure. Paul earned his M.S. in Homeland Security Management from the Homeland Security and Terrorism Institute at LIU Post, and holds a B.A. in Homeland Security & Emergency Management from Ashford University. As an active member in the academic, security and emergency management communities, Paul serves as the Advisory Board Chair and Executive Director of the Homeland Security and Security Management program at the Long Island Business Institute in New York. He also serves as an Adjunct Professor under the U.S. Department of Homeland Security–Transportation Security Administration Partnership Program at Erie Community College.