Scholar Chatter, Volume 2, Issue 1, March 2021
ISSN 2692-8426 (online)

THE EFFECTS OF SOCIAL ENGINEERING ON ENTERPRISE SECURITY

Author ORCID: https://orcid.org/0000-0001-6140-236X

Author Affiliation: Taurus J. Jackson, DM/IST, University of Phoenix, Phoenix, Arizona

SC Classification Genre: Business

Citation: Jackson, T. J. (2021) The effects of social engineering on enterprise security. *Scholar Chatter*, *2*(1), 1–14. http://doi.org/10.47036/SC.2.1.1-14.2021

Abstract

The focus of this research was to explore present control methods and solutions used throughout technology-based, healthcare-based, and manufacturing-based organizations in southwest Georgia to determine their effectiveness for reducing potential threats. Semi-structured interviews with open-ended questions are used to explore 30 information technology professionals' lived experiences with IT security policies and procedures. Two research questions guided the qualitative exploratory case study: How important is social engineering and enterprise security to the organization? and How are organizations evaluating and managing existing organizational solutions? Several themes emerged: (a) lack of education and inadequate information can affect the decision-making process, (b) response times from management is a key factor in reducing threats, (c) a sense of failure is always present, (d) failed IT policy management can increase organizational vulnerability, and (e) social engineering still has a negative stigma in the business environment. The findings suggest that although steps were made to change the perception of social engineering and enterprise security, additional work is needed to ensure employees are aware of how social engineering and enterprise security can affect their organization productivity.

Key Words: *Information systems, information technology, social engineering, enterprise security, control methods, policies, procedures, management*

Introduction

Social engineering and enterprise security continue to be significant because organizations progressively have observed a vulnerable link exists in the security chain (Bongiorno et al., 2018). Without employing risk mitigation controls, many organizations would be unable to monitor well-known threats, recognize new threats, and gauge existing processes effectively (Kumaresan et al., 2017). Therefore, demonstrating why organizations are apprehensive about integrating external applications and services into their existing organizational infrastructure (Janssen et al., 2017). Organizations should prioritize information system platforms that would allow them to offer enhanced functionality while identifying potential threats and increasing security awareness (Ki-Aries & Faily, 2017). The purpose of this research was to explore present control methods, solutions, and vulnerability identification methods used throughout technology-based, healthcare-based, and manufacturing-based organizations in southwest Georgia related to reducing potential threats and information systems vulnerabilities

Recent incidents such as the WikiLeaks scandal exemplify the need for additional vigorous human-centric enterprise security measures to remediate risks associated with social engineering and enterprise security (Brinkman et al., 2020). Preventing social engineering attacks remains a challenge for most organizations (Mittelstadt, 2017; Vinaja, 2020). Thus, highlighting that some organizations do not have adequate solutions in place to protect organizations against social engineering attacks like identity theft or breach in enterprise security (Rocha Flores & Ekstedt, 2016). Social engineering attacks compromise enterprise security in a susceptible way within any information security infrastructure, organization, or its professionals. Therefore, successful social engineering attacks enabled the attacker to circumvent millions of dollars devoted to technical and nontechnical protection devices and consulting, completely nullifying security investment (Schmidt, 2016).

One of the fundamental problems with analyzing, understanding, managing, and combating social engineering attacks lies within the way in which organizations managed access and security control methods. Organizations were analyzing social engineering from a historical perspective which sought to improve current data management processes to making recommendations for preventing future attacks (Chaudhry et al., 2016). Despite advances in technology to protect data loss, data breaches continued to occur within the organization thus jeopardizing unclassified and classified information. The average cost of social engineering attacks for employees can range from $25,000 to $100,000 dollars per attack and cost the organization on average $66.9 million dollars annually (Junger et al., 2017). Effectively identifying and integrating enterprise security endeavors seems an intimidating task because many endeavors fail or are not properly executed (Hoogervorst, 2017).

Literature Review

The conceptual framework for this paper was based on the social engineering defensive framework (SEDF). Organizations and employees view social engineering and enterprise security as being an important concept but may not realize the extensive damage an attack can

have on the organization (Schaab et al., 2017). A major misconception about social engineering and enterprise security indicates one is more important than is the other. Consequently, both social engineering and enterprise security are addressed before organizations can explore current solutions and propose new solutions.

The SEDF attempts to provide organizations with a method of assessing general and specific business, technology, and security concerns (Chen, 2017). Although the SEDF is implemented throughout organizations, its implementation is unique to each organization. Results from each social engineering assessment can result in similar responses from organizations and employees. The SEDF is comprised of four phases: (a) determining exposure, (b) evaluating defenses, (c) educating the workforce, and (d) streamlining existing IT policies (Satapathy & Jenila Livingston, 2016). Each phase of the SEDF is executed in any order and not dependent on a previous phase or the next phase. Misunderstanding of social engineering and enterprise security continues to be problematic for technology, manufacturing, and healthcare organizations (Tuma et al., 2018). To provide clarity of social engineering and enterprise security, organizations should carefully explore the SEDF to reduce potential attacks (Eizenberg & Jabareen, 2017).

To reduce potential attacks, organizations should focus on the larger picture and involve key business and technical members from multiple departments inside and outside the organization (Singh & Sidhu, 2015). As a result, this allows organizations to receive input from employees who perform actual duties regularly. The conceptual framework of this paper was used in a way to help organizations and employees to understand social engineering, enterprise security, and the impact it may have on the organization, if not properly addressed

The review of literature indicated a gap in knowledge relating to the historical aspect of social engineering and enterprise security, effective organizational control methods, solutions, and educational awareness for employees regarding potential threats (Suganya, 2016). Studies outlined the complex nature of social engineering and enterprise security but have not fully explored the value each component could provide an organization. Moreover, the review of literature facilitates discussions on the characterization of a social engineer, explanations of the social engineering and design process, and what social engineers do (Marczak & Paxson, 2017). Even though Weaver, Furr, and Norton (Wardono et al., 2017) outlined a convenient historical perspective of engineering ethics, inconsistencies still exist pertaining to what social engineers do. Each of these subjects details the exchanges between an engineer and other individuals such as employers, employees, and other partners in the IT profession (Li et al., 2018).

Methodology

A qualitative exploratory case study was used to explore present control methods and solutions used within the organization to determine the overall effectiveness. I explored issues related to social engineering and enterprise security and sought to provide answers as to the why and how type of questions. The population comprised 30 full-time or part-time employees; IT professionals ranging from the helpdesk to the information assurance in technology-based, healthcare-based, and manufacturing-based organizations in southwest Georgia. Additional

demographic characteristics collected were age, gender, organizational location, organizational type, educational level, clearance level, and user account type.

Sample

A nonprobability sampling was beneficial for the qualitative exploratory case study. Using a convenience sampling design was more appropriate because it was based on participants' willingness to take part (Thorne, 2020). The human resources department of each of three organizations participating in the study representing technology-based, manufacturing-based, and healthcare-based was contacted by email or phone with a request for permission to conduct the study. After each organization provided signed permission, they were provided with the purpose of the study and criterion for participant participation via the recruitment email. The criterion for selecting participants was to be 18 years or older, to work or have worked at either a technology-based, manufacturing-based, or healthcare-based organization for 10 years, to hold or have held a security clearance, to hold or have held an administrative or user access, and to be a current or former employee of the organization.

Instrumentation

Validity and Reliability

Data or information on the validity of case study instruments and data gathering techniques reflected an interpretive method that illustrates participants' experiences and viewpoints to create meaningful stories (Nicho, 2018). External respondents were asked to analyze and review instrumentation-related information to ensure relevancy and reliability. Expert external reviewers included college professors, IT managers, data entry specialists, and former doctoral students. The process involved face-to-face conferences, expounding, and collaborating on the conceptual framework, research questions, survey questions, data analysis, and data integration.

Data Triangulation: Reinforcing Validity

Triangulation was achieved by reviewing and analyzing interview transcripts, survey responses, and field notes. I also applied theoretical processes, like the social engineering defensive framework, to validate participant accuracy. Member checking was used to triangulate and improve the validity of the data (Noble & Heale, 2019).

Data Collection

The arrangement of interviews, emails, and surveys was based on accessibility of participants. In addition, the data collection process allowed me to gather accurate information from participants in the study. Interviews were based on preferred location of participants. Each participant's completion timeframe varied, depending on the level of experience, amount of information provided, and the level of involvement pertaining to interviews and surveys. Interviews and surveys were planned and formulated to acquire necessary data that research needed when using open-ended questions. I asked 30 research participants to partake in the exploratory case study by either face-to-face, phone, or email. Research participants consented to a part of the research and met specific criteria Participants answered questions in-person or

through electronic surveys. Interviews or surveys were conducted for the duration of 45 minutes to an hour in which I documented all responses to identify specific themes and patterns in responses. Research data were manually and electronically collected using the combination of a written copy of the interview or survey responses, a digital recorder, and smartphone and analyzed responses for accurateness. Because of the nature of the study, certain interview or survey questions were considered stressors. If participants considered a question to be a stressor, he or she was able to contact his or her local counseling services department for support or withdraw from the study.

Each participant obtained an explanation about the survey, its purpose, confidentiality, benefit, schedule, risk, and who was involved. After participant involvement was obtained, they either received interview or survey questions via an email attachment or a hard copy along with a schedule completion deadline for the survey or interview to complete and return. Participants who agreed and arranged to meet in person received face-to-face interviews, and participants who were not able to meet face-to-face but wanted to participate in the research study received a survey as an email attachment. Interaction with participants allowed me to redefine previously asked questions during successive interviews. No limit was placed on the number of responses for interview questions. However, there was a limit placed on the number of choices or responses for the survey. The survey contained five options participants could select. Surveys were used to collect data and included a Likert scale that used positioning statements. Qualitative data were collected on a daily or weekly basis and reviewed frequently to ensure the data collection process was performed accurately. After interviews or surveys were completed, responses were logged and tracked via a coding system. Alpha-numeric pseudonyms to identify participant information was used for analysis during the study.

Data Analysis

The intention of this exploratory case study was to explore present control methods and solutions used throughout technology-based, healthcare-based, and manufacturing-based organizations in southwest Georgia to determine their effectiveness for reducing potential threats. Participant's replies were analyzed to classify themes and patterns relevant to each research question developing from the data. Data compiled from interviews and surveys were divided into individual perceptions and organizational perceptions. This preliminary classification was accomplished for data organization. The concluding stage of analysis emphasized combined perceptions of individuals and organizations and provided insight into social engineering and enterprise security.

Planning for data analysis involved gathering data from participants of the study, transferring data were manually and electronically collected using the combination of the written copy interview or survey responses, a digital recorder, and smartphone then organizing data using Microsoft Excel, and formatting data for exploration. Once documents were formatted for consistency, five themes and patterns pertinent to research questions developed from the data. The software offered users the chance to explore crucial words or phrases and classify replies according to those words or phrases thus generating data sets. Furthermore, organizing words or

phrases further produced major or minor themes related to social engineering and enterprise security.

Findings

The research study explored present control methods and solutions used throughout technology-based, healthcare-based, and manufacturing-based organizations in southwest Georgia to determine their effectiveness for reducing potential threats. In particular, the qualitative exploratory case study explored two main research questions relating to social engineering, enterprise security, and information systems vulnerabilities:

RQ1: How important is social engineering and enterprise security to the organization?

RQ2: How are organizations evaluating and managing existing organizational solutions?

Significant Study Findings

Social engineering and enterprise security was an important factor for each organization and their respective IT and managerial personnel. Although each organization and their respective IT and managerial personnel may not have a clear understanding of social engineering or the social engineering process, many of them recognize and understand that enterprise security plays an essential part in protecting organization's information systems. Study findings from the case study highlighted the role of social engineering, enterprise security, the positive or negative outcome of social engineering, and enterprise security, and revealed how well IT and managerial personnel across multiple organizations understood the overall social engineering process. While organizations and their employees in the case study realized social engineering had the potential to present major issues, through research findings, it was illustrated that some organizations did not know how severe those issues could impact their organization's information systems.

Core Themes of the Study

Exploring organizations' experiences and perceptions about social engineering and enterprise security might allow organizations to address inconsistencies with present control methods and solutions to determine the effectiveness for reducing potential threats accurately. Data compiled from interviews and surveys were divided into individual perceptions and organizational perceptions. The data analyzed from conducting the study resulted in five core themes: (a) lack of education and inadequate information can affect the decision-making process, (b) response times from management is a key factor in reducing threats, (c) a sense of failure is always present, (d) failed IT policy management can increase organizational vulnerability, and (e) social engineering still has a negative stigma in the business environment.

Theme 1. Lack of Education and Inadequate Information can Affect the Decision-Making Process

Research participants demonstrated minimal knowledge of the social engineering process and enterprise security. Research participants also demonstrated with adequate information, organizations might be able to address social engineering and enterprise security issues properly. Further, research participants provided their experiences with the social engineering process and

enterprise security. In conjunction with the study's conceptual framework, particularly with one of the phases explored educating personnel, was a key component to addressing issues with understanding the social engineering process and enterprise security. The review of the literature supported findings regarding the importance of understanding the social engineering process and organizations providing adequate information to their employees. Study results illustrated many individuals do not have a clearly defined view of social engineering but do have a clearly defined concept of enterprise security.

Contrary to data presented in the research study and the general perception of social engineering and enterprise security, individuals and managers have conflicting knowledge of social engineering and enterprise security. Based on research findings, individual and managerial viewpoints of social engineering and enterprise security across organizations generated similar responses but did not present standardized viewpoints. Furthermore, individuals and managers across organizations were split as well, which further indicates the perception of the social engineering process and enterprise security is not well defined. The lack of education and inadequate information could decrease an organization's ability to reduce potential attacks.

Theme 2. Response Times from Management is a Key Factor in Reducing Threats

Research participants indicated response times from management was a key factor in reducing threats. The response time related to managing social engineering issues has amplified intensely thus decreasing the efficiency of acceptable response times (Yuan et al., 2020). It is very important for various organizations to evaluate their response times relating to identifying and testing social engineering solutions. Because there is a lack of evidence surrounding proposed solutions, performing a threat analysis to pinpoint and verify potential targets of an attack would have little to no effect on mitigating social engineering risks (Shi, 2019). Four of nine individuals felt strongly about current solutions used. On the other hand, the other five individuals were again split on their assessment related to current solutions used. Two individuals felt current solutions used were efficient, two individuals felt current solutions were moderately efficient, and one individual was not sure about current solutions used.

While individuals felt similar in their assessment of current solutions used throughout each organization, there is work needed to standardize current solutions used throughout the organization in an attempt to provide pre-preventative actions. Granted improvement was made; management from each organization must be more involved in managing social engineering issues and evaluating current solution

Theme 3. A Sense of Failure is Always Present

Despite organizations wanting a sense of consistency relating to combating social engineering attacks, a sense of failure is always present. One of the most vital steps in combating social engineering is to inspect an organization's preparedness levels (Anson et al., 2017). Research participants openly expressed their frustration with their organizations not showing preparedness and being inconsistent when it came to managing social engineering and enterprise security issues. Among responses received from individuals from the technology-based organization, the confident and unconfident responses received the exact number of responses,

three each. This further demonstrates the complexity of social engineering across organizations. Furthermore, research participants stated managing enterprise security was equally important to each organization. Although research participants indicated there was cohesiveness among some organizations, results from the study prove standardization is not common across organizations.

Theme 4. Failed IT Policy Management can Increase Organizational Vulnerability

Research participants indicated organizations should establish, implement, and manage appropriate IT policies and procedures. An overwhelming number of individuals from all three organizations indicated to combat social engineering and enforce enterprise security, one must be familiar with their organization's policies related to protecting information systems. Three out of five individuals viewed policies related to protecting information systems as effective. Based on data analysis, five out of 12 individuals viewed policies related to protecting information systems as being moderately effective. The other seven individuals were split in their assessment of this topic. Policy inconsistences are still a major concern for individuals from all organizations. Conversely, many individuals viewed current monitoring policies or best practices favorably, there were some individuals who did not view their organization's current monitoring policies or best practices as being effective.

Even though there was indecisiveness among individuals regarding IT policy management, the gap began to lessen as more individuals began to agree on various social engineering elements and provided a more definitive viewpoint. As a result, research participants noted a shift across organizations continues to grow and thus, social engineering and enterprise security is slowly gaining the same attention. Furthermore, research participants suggested the failure of IT policy management results from a lack of strategic planning. Research participants reorganized restricted resources and evolving roles managers have in daily operations allows less time for strategic planning.

Theme 5. Social Engineering Still has a Negative Stigma in the Business Environment

Research participants indicated having minimal to marginal knowledge of how social engineering affects the organization. Among various organizations, individuals from all organizations viewed business environment severity as being very severe. Out of all participants, one individual felt social engineering could have a very severe impact on the business environment and six individuals felt social engineering could have a severe impact on the business environment. Three individuals felt social engineering could have a moderately severe impact on the business environment, one individual felt social engineering did not have a severe impact on the business environment, and one individual was not sure how severe social engineering could impact the business environment. Individuals from all organizations also felt very strong about the financial and operational risks associated with social engineering and enterprise security. Findings provide a fully structured, clearly stated, report of the results of the research.

Discussion

Existing research indicated social engineering was a process that could be a simple or complex issue, depending on the method used by the social engineer. Within the literature, alternative solutions were introduced to individuals from various organizations on concepts related to social engineering, enterprise security, and how to combat or reduce information system vulnerabilities. Responses from individuals implied that although steps were made to change the perception of social engineering and enterprise security, additional work is needed to ensure more individuals are aware of the lasting impact social engineering and enterprise security has on their organization. Responses from individuals also implied identifying potential social engineering-related threats does not necessarily reduce information systems vulnerabilities in organizations. While all organizations in the research study viewed social engineering and enterprise security as very important, the healthcare-based organization exhibited the greatest mixed results, when compared to the other organizations in the research study. Topics ranged from having poor response times related to identifying and testing social engineering solutions to evaluating the efficiency of organizational solutions. However, as the study process continued, the healthcare-based organization began to have several shifts but soon shifted back to its original position as being indecisive in their viewpoint of social engineering and enterprise security.

To further highlight issues for individuals from the healthcare-based organization, individuals were not familiar with the social engineering process. Subsequently, since the healthcare-based organization manages various type of information, such as an individual's demographic data, past, current, or future mental conditions, which are governed by HIPAA of 1996, not many individuals from this organization were familiar with the social engineering process. This response received the highest reaction with four responses. Existing research further indicated because there is a lack of evidence surrounding proposed solutions, performing a threat analysis to pinpoint and verify potential targets of an attack would have little to no effect on mitigating social engineering risks. Individuals from all organizations indicated while current solutions were viewed as efficient or moderately efficient, individuals understood no specific solution alone could reduce potential social engineering-related threats or reduce information systems vulnerabilities. Responses from individuals implied that although steps were made to explore benefits of current organizational solutions and the direct impact they have on identifying social engineering-related threats, additional work is needed to ensure current organizational solutions are enhanced and advanced solutions are created and implemented in their organization.

Implications to Practice

After conducting in-depth research and evaluating gathered data, organizations in the research study continue to use current organizational solutions but shift the focus to strengthening the efficiency of those solutions while advancing and expanding organizational solutions aimed at circumventing or reducing social engineering-related threats. Based on research findings from the previous literature review and case study participants, it may be important for organizations to develop more aggressive techniques to ensure individuals not only

are introduced to social engineering and enterprise security but also have a comprehensive perspective of the concept.

Including more aggressive processes would allow organizations to provide direction to strengthen a culture of operational security concerning social engineering and enterprise security. Furthermore, this would also allow organizations to develop stricter information technology policies and policy management tools to enhance or promote better organizational communication and policy-making decisions. Enhancing IT policy management would permit organizations to reevaluate the efficiency of current organizational solutions to determine pros and cons of those solutions and to test those solutions further for maximum potential efficiency. From the research study, it may be important for organizations to consider hiring individuals who are familiar with ethical hacking techniques. Currently, the industry-required certification to operate an organization's information system is Security+. By requiring potential employees to acquire ethical hacking certification, this may allow potential employees to focus on vulnerability testing and better securing an organization's information system

The healthcare-based organization might consider establishing more advanced online certificate producing courses available to not only IT personnel but to personnel from other units of the healthcare-based organization. Training resources are linked to the organization's Training Command Center (TCC) via the organization's Learning Management System (LMS). Each unit should establish training managers certified to not only address healthcare-related issues but also social engineering issues and provide personnel with resources to contact external assistance, if necessary, to streamline the process effectively. Additionally, designing, enhancing, or promoting the organization's website could serve as a central focal point. This website will feature healthcare-related historical, existing, and future website links accessible for training and informing employees about social engineering, enterprise security, and information systems vulnerabilities. Currently, there is no specific industry-required certification to operate an organization's information system. Therefore, more healthcare-based organizations are beginning to ask current or potential information technology staff to acquire the Health Care Information Technology Certificate (HCITC), which is not yet a standard. By requiring potential employees to acquire the HCITC, it will allow potential employees to focus on vulnerability testing and better securing an organization's information system and healthcare medical records.

Future Research

Because of the findings, it is clear organizations will continue to adjust to numerous encounters surrounding social engineering, enterprise security, and information system vulnerabilities. This exploratory case study may serve as a basis for additional studies. One recommendation for future research is to further explore and comprehend the complexity of the organizational environment of each organization to see how or if social engineering, enterprise security, and information system vulnerabilities are addressed. As seen in previous and current research studies, just because concepts of social engineering, enterprise security, and information system vulnerabilities are discussed by one organization does not mean those discussions or issues are transferrable to different organizational types. Another recommendation is to determine how individuals in larger geographical locations perceive social engineering,

enterprise security, and information system vulnerabilities. How individuals obtain access to an organization's information system deserves exploration, since larger geographical groups tend to have more employees when compared to small and midsized organizations. Although steps were made to change the perception of social engineering and enterprise security, additional work is recommended to ensure more individuals are aware of the lasting impact social engineering and enterprise security has on their organization

From an additional qualitative perspective, future researchers might conduct a descriptive case study. A descriptive case study might provide insight into how corrective solutions were properly implemented not only within a specific organization but also across multiple organizations concurrently. Descriptive research might also focus on why corrective solutions did not occur. In addition, an appropriate quantitative methodology might also be useful to conduct future research. Quantitative researchers might use a comparative study to inquire if corrective solutions fluctuated over a specific timeframe. Moreover, quantitative researchers could use the results from this study to form hypotheses to inquire about the possible effectiveness of each method and the possibility of inquiring what methods worked towards preventing future threats and attacks within organizations.

Conclusion

Data from this exploratory case study came from 30 IT professionals and managerial personnel across functional areas, ranging from the help desk to information assurance and security personnel, in an attempt to explore what safeguards and solutions are in place relating to protecting organizational data and enterprise security. Five themes emerged from data gathered during data analysis process. Responses reinforced the notion that social engineering, enterprise security, and information system vulnerabilities was still an issue despite the advancement of organizational solutions currently used throughout various organizations. Responses from individuals implied that steps were made to change the perception of social engineering and enterprise security, additional work is needed to ensure more individuals are aware of the lasting impact social engineering and enterprise security has on their organization.

Results of this exploratory case study indicated social engineering and enterprise security remains an important topic of discussion for organizations. This further illustrated individuals throughout all three organizations misunderstood social engineering and enterprise security. While inadequate and conflicting information is sometimes presented to employees along with the lack of standardization across multiple organizations and platforms, organizations have attempted to have a more focused presence when addressing social engineering and enterprise security issues. Because social engineering still has a negative stigma in the business environment, organizations realize this must be properly managed before implementing corrective measures to reduce potential attacks. Based on emerging themes, IT management and personnel must invest in, implement advanced organizational solutions, and have a rich understanding of social engineering and enterprise security to combat existing threats and reduce potential threats.

Funding

The author received no financial support for the research, authorship, and/or publication of this article.

Acknowledgements

I would like to acknowledge all my past facilitators from the University of Phoenix. They laid the foundation for my doctoral journey and were supportive of all my decisions related to pursing Masters and Doctoral Degrees. Dr. Greenfield, I would like to thank you for your support and guidance through this process. Dr. Bunn, Dr. Fonseca-Lind, Dr. D'Angelo, and Dr. Talbert, I would like to thank you for allowing me to lean on your expertise for guidance and showing me alternate ways of getting through the process. I would also like to thank Dr. Julie Conzelmann for providing great advice as an editor and reviewer.

References

Anson, S., Watson, H., Wadhwa, K., & Metz, K. (2017). Analysing social media data for disaster preparedness: Understanding the opportunities and barriers faced by humanitarian actors. *International Journal of Disaster Risk Reduction, 21*, 131–139. https://doi:10.1016/j.ijdrr.2016.11.014

Bongiorno, C., Rizzo, A., & Porfiri, M. (2018). An information-theoretic approach to study activity driven networks. *2018 IEEE International Symposium on Circuits and Systems (ISCAS)*. https://doi:10.1109/iscas.2018.8351825

Brinkman, C. S., Gabriel, S., & Paravati, E. (2020). Social achievement goals and social media. *Computers in Human Behavior, 111*, 106427. https://doi:10.1016/j.chb.2020.106427

Chaudhry, J. A., Chaudhry, S. A., & Rittenhouse, R. G. (2016). Phishing attacks and defenses. *International Journal of Security and Its Applications, 10*(1), 247–256. https://doi:10.14257/ijsia.2016.10.1.23

Chen, J. Q. (2017). A new dynamic cyber defense framework. *International Journal of Cyber Warfare and Terrorism, 7*(4), 14–22. https://doi:10.4018/ijcwt.2017100102

Eizenberg, E., & Jabareen, Y. (2017). Social sustainability: A new conceptual framework. *Sustainability, 9*(1), 68. https://doi:10.3390/su9010068

Hoogervorst, J. (2017). The imperative for employee-centric organizing and its significance for enterprise engineering. *Organizational Design and Enterprise Engineering, 1*(1), 43–58. https://doi:10.1007/s41251-016-0003-y

Janssen, M., van der Voort, H., & Wahyudi, A. (2017). Factors influencing big data decision-making quality. *Journal of Business Research, 70*, 338–345. https://doi:10.1016/j.jbusres.2016.08.007

Junger, M., Montoya, L., & Overink, F.-J. (2017). Priming and warnings are not effective to prevent social engineering attacks. *Computers in Human Behavior, 66*, 75–87. https://doi:10.1016/j.chb.2016.09.012

Ki-Aries, D., & Faily, S. (2017). Persona-centered information security awareness. *Computers & Security*, *70*, 663–674. https://doi:10.1016/j.cose.2017.08.001

Kumaresan, T., Saravanakumar, S., & Balamurugan, R. (2017). Visual and textual features-based email spam classification using S-Cuckoo search and hybrid kernel support vector machine. *Cluster Computing*, *22*(S1), 33–46. https://doi:10.1007/s10586-017-1615-8

Li, Z., Chu, T., Kolmanovsky, I. V., Yin, X., & Yin, X. (2018). Cloud resource allocation for cloud-based automotive applications. *Mechatronics*, *50*, 356–365. https://doi:10.1016/j.mechatronics.2017.10.01

Marczak, W. R., & Paxson, V. (2017). Social Engineering Attacks on Government Opponents: Target Perspectives. *Proceedings on Privacy Enhancing Technologies*, *2017*(2), 172–185. https://doi:10.1515/popets-2017-0022

Mittelstadt, B. (2017). Designing the health-related internet of things: Ethical principles and guidelines. *Information*, *8*(3), 77. https://doi:10.3390/info8030077

Nicho, M. (2018). A process model for implementing information systems security governance. *Information & Computer Security*, *26*(1), 10–38. https://doi:10.1108/ics-07-2016-0061

Noble, H., & Heale, R. (2019). Triangulation in research, with examples. *Evidence Based Nursing*, *22*(3), 67–68. https://doi:10.1136/ebnurs-2019-103145

Rocha Flores, W., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security*, *59*, 26–44. https://doi:10.1016/j.cose.2016.01.004

Satapathy, A., & Jenila Livingston, L. M. (2016). A comprehensive survey of security issues and defense framework for VoIP Cloud. *Indian Journal of Science and Technology*, *9*(6), 1-13. https://doi:10.17485/ijst/2016/v9i6/81980

Schaab, P., Beckers, K., & Pape, S. (2017). Social engineering defence mechanisms and counteracting training strategies. *Information & Computer Security*, *25*(2), 206–222. https://doi:10.1108/ics-04-2017-0022

Schmidt, P. (2016). Communities and workforce development. *Community Development*, *47*(5), 747–748. https://doi:10.1080/15575330.2016.1230304

Shi, Z. (2019). Optimal remanufacturing and acquisition decisions in warranty service considering part obsolescence. *Computers & Industrial Engineering*, *135*, 766–779. https://doi:10.1016/j.cie.2019.06.019

Singh, S., & Sidhu, J. (2015). An approach for determining trustworthiness of individuals in a web-based social network. *Arabian Journal for Science and Engineering*, *41*(2), 461–477. https://doi:10.1007/s13369-015-1656-3

Suganya, V. (2016). A review on phishing attacks and various anti phishing techniques. *International Journal of Computer Applications*, *139*(1), 20–23. https://doi:10.5120/ijca2016909084

Thorne, S. (2020). Beyond theming: Making qualitative studies matter. *Nursing Inquiry*, *27*(1). https://doi:10.1111/nin.12343

Tuma, K., Calikli, G., & Scandariato, R. (2018). Threat analysis of software systems: A systematic literature review. *Journal of Systems and Software*, *144*, 275–294. https://doi:10.1016/j.jss.2018.06.073

Vinaja, R. (2020). The world IT project global issues in information technology. *Journal of Global Information Technology Management*, *23*(4), 329–330. https://doi:10.1080/1097198x.2020.1834077

Wardono, P., Hibino, H., & Koyama, S. (2017). Effects of restaurant interior elements on social dining behavior. *Asian Journal of Environment-Behaviour Studies*, *2*(4), 43–53. https://doi:10.21834/aje-bs.v2i4.209

Yuan, X., Olfman, L., & Yi, J. (2020). How Do Institution-Based Trust and Interpersonal Trust Affect Interdepartmental Knowledge Sharing?. In Management Association, I. (Ed.), *Information Diffusion Management and Knowledge Sharing: Breakthroughs in Research and Practice* (pp. 424-451). IGI Global. http://doi:10.4018/978-1-7998-0417-8.ch021