



Human Factors in Information Assurance: A Review of Behavioral and Cultural Aspects

Nahid Neoaz

Wilmington University, USA

nahidneoaz@yahoo.com



*Corresponding Author

Article History:

Submitted: 25-12-2024

Accepted: 25-12-2024

Published: 30-12-2024

Keywords: Information security, psychology, cultural psychology, computer security, social engineering, compliance, positive organizational culture, security, heuristic errors, individual differences, two factor authentication, security operation standards, leadership, and risk analysis

Brilliance: Research of Artificial Intelligence is licensed under a Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0).

ABSTRACT

IA is a critical field in shielding information and information structures from unapproved use, divulging, interference or demolition. Technical controls applied in IA provide ways of preventing such acts and managing the risk but since aspects of operational environment and people's attitudes significantly influence IA as an exercise, it represents a critical factor. This paper on IA focuses on behavior and culture that affect human decision making process, Cognitive Bias, and emotions, security behaviors and structures. It addresses the aspect of how a user will prefer convenience to security, get to provide information to an unauthorized user and or will not follow most organizational policies due to ignorance of the detected securities put in place. The final factors that the paper analyses as the factors influencing security within an organization include leadership engagement, training, security awareness and security culture. Lastly, information is presented about social engineering as an attack approach as well as measures to prevent them, such as, for example, using multi-factor authentication. The paper insists that strategy for IA cannot do without including technical solutions as well as a consideration of regard human behavior and practice as a method of unfolding a security culture across organizations. In addition, by applying the evaluation framework in this paper, organizations enhance on technical and human IA approach, and reduce risk elements, familiarize people with new hostile forces emerging to threaten secret information.

INTRODUCTION

Information Assurance can also be defined as the protection of information including methods of processing, storage, disposal and communication to ensure confidentiality, integrity, availability, authenticity and non-repudiation. It embraces all the preventive factor from the tools and measures in the worried information system and the principles, processes and systems that are implemented to counter the threats of misuse, computer criminal activities, breaches and viruses among others. , technical definitions and has been described in the past referring to systems, defending, shielding, encrypted, networks. But the usage of the human factor has suddenly appeared as one of the key drivers of goals concerning the protection of information and assets [1]. The concept of people as being fundamental within IA stems from the fact that, for instance, there are often rigid technologies that are quite effective in providing profound security insurance with low levels of complication; however, people are the weakest links. Alone through such clusters that are created by the techniques of unskilled workers, it is possible to explain a major part of all cyber security incidents familiar to a company, including data leakage and system intrusions. Thus, referring to the classification of different categories of activities and risks for IA, it is necessary to state that the issue cannot be solved only with technical provisions, but requires their assessment together with the appropriate behavioral and cultural factors [2].

More specifically, this paper aims at assessing behavioral and cultural aspects of IA in order to understand how human behavior, decision making and organizational cultures shape security outcomes. The purpose of this particular work is to present the current understanding of the approaches of human engagement in IA with emphasis on psychological characteristics of exposure and social and cultural aspects of secure and insecure behaviors [3]. From these dimensions, the paper will identify major trends that have to be built or unbuilt to make expansion of IA possible for improvement through human centered frameworks. The focus of this review will also include factors such as; user awareness, personal inclinations when it comes to matters concerning security, social engineering attacks carried out on individuals/groups within an organization, organizational culture as either an enabler or a detractor when it comes to adoption of measures/tutorials relative to security [4]. The paper is to underscore when speaking about IA, it is the function which should be protected not only by means of modern technologies but also taking into account impact of human factors into the further information protection in the world turning into one big network [5].

Fundamental notion of Information Assurance

IA also notes that the behavioral factors contribute greatly to system behavior since these are the real dynamics in managing the security system, polices and protocols. More often than not, one gets to determine whether to follow or not



to follow security measures out of one's rational and prefrontal cortex, or being hasty and risking endangered info, depending on one's mood and learning. It is essential for this for its realization indicating successful IA strategies do not employ solely technical aspects, but also pay attention to the processes occurring in cognition of a person who is a threat in terms of IT security [6]. A critical behavioral concern inherent in IA is an explanation of security determinations that individuals make. Research has shown that people are likely to take decisions based on what they consider easiest rather than what would best secure them. For example, an easily memorable password, the deficiency of which is compensated for by a high entropy, or users investing substantial time to bypass security measures [7]. Such behaviors are normally as a result of the genetic fallacy referred to as "security fatigue" whereby the application users become either bored or care free due to continued alerts and are more often than not blinded by the ease of use of the applications [8].

There are also emotions that IA decision making and these are fear, anxiety and overconfidence. A raw kern with limited inputs on phishing may eagerly jump into action of needful email as if it's an emergency or lacking proper founders. On the other hand he/she who too confident of his/her ability to ward-off cyber threats May equally disregard the required security precautions saying he/she cannot be attacked or hacked. These emotional responses tend to make one not very reasonable or else set a considerably easy target for a security breach [9]. One of the biggest behavior problems is the absence or inadequate information in matters concerning security. However, a vast number of users are not familiar with all types of threats in the informational world, so one can become a victim of cybercriminals. Such lack of knowledge is even complemented by weak or inefficient security awareness training regimes available. As the best practice research reveals the awareness campaigns with the exclusively technical appeals are not as effective as the ones which tell people the reasons for their actions in terms of psychology and social influence [10].

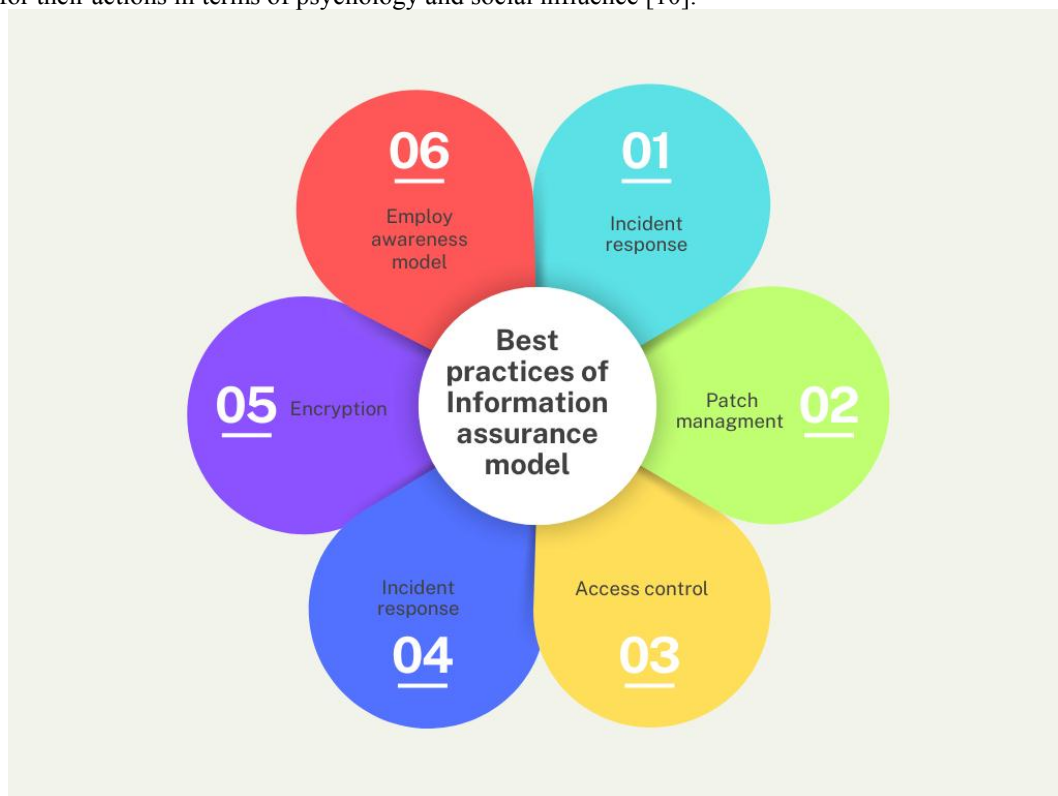


Figure: 1 showing rest practices of information assurance model

It may also cast more light into how boosting IA may be achieved further through mode of behavioral change. Assuasive tools targeting behavioral change among which are nudging, a solution wherein people are given hints to turn towards safer choices while staying free to make the choice, can prove to be quite useful when it comes to inducing safer behaviors. Especially notification like default settings that requires two factor authentication or when passwords are to be changed can force the users to adopt reasonable practices [11]. Incorporation of gasification in security awareness programs improves the latter because more individuals participate in them and can readily remember what has been taught without cues. By this we discovered that dealing with the behavioral dynamics that define IA requires a complex procedure. It goes further than simply telling users what kind of threats are out there and how to beware of them, but also how to create infrastructure and include elements from psychology which actively encourage secure behaviors [12]. Minimizing reliance on fallible human appraisals thus the potential for human-generated vulnerability for fire personal data, organizational information assurance can be improved by eliminating the sources of bias that underpin decision making and controlling for the streams of emotion that motivate individuals [13].

INFORMATION ASSURANCE AS VIEWED FROM CULTURAL ANGLE

The cultural factors thus assume the highest significance in defining IA and how organizations manage security of their information and how people regard and act on the steps taken towards protecting information that is strategic to an organization. Moreover, it critically plays an even more essential role while identifying the activities, attitude and policies to be followed regarding information protection measures and that is, corporate culture, cultural norms and business culture [14]. Therefore, understanding of the actual Cultural IA elements is necessary in order to obtain the good set of the contextually adequate and effective IA strategies that would contribute to the establishment of the security-aware environment. On the last level, culture that is security conscious will ensure that the employees are as far as handling sensitive data and security measures and policies are concerned is very important at the organizational level [15]. This seems to be the case due to its top-down approach and managers and leaders have the major responsibility of cultivating this aspect of security in organizations. This predicative study assumed that when top management shares the vision of information security, contributes by providing funding for security for improvement and set the anticipated level of adherence it becomes easier for the employees to embrace the security measures and procedures require to support information security. On the other hand, weak leadership commitment to IA from the executives might result in promoting organizational security as an afterthought [16].

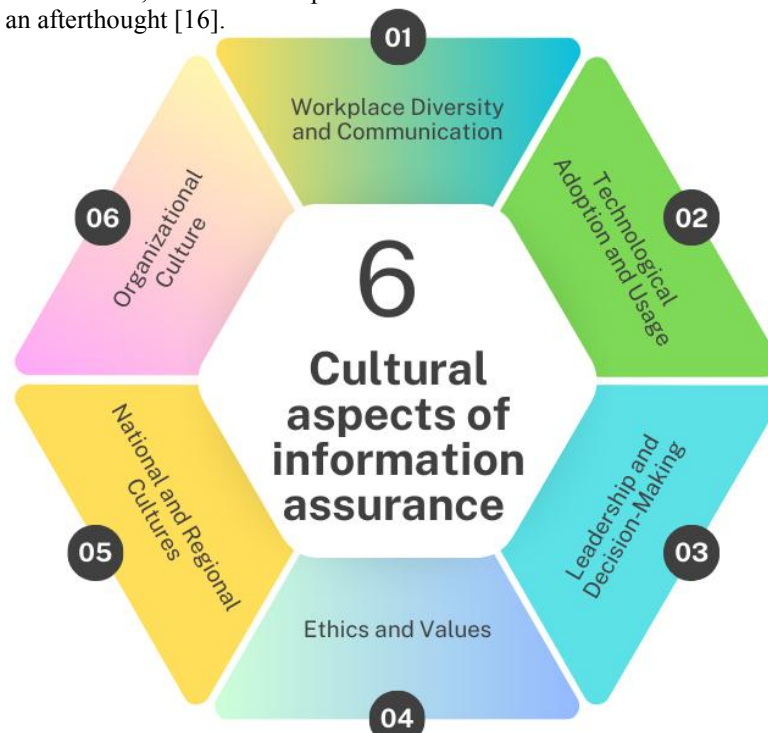


Figure: 2 showing cultural aspects of information assurance

In addition, there are effects on organization culture on the experiences of employees perceiving and engaging security policies. For instance in some organizations there is usually a culture of 'risk taking' and people will continue to work without observing security measures and taking their time. In such cultures institutions and measures of security can be seen as inhibitors rather than as enablers [17]. On the other hand, the study reveals that companies that embrace security consciousness receive better compliance with the policies like password update, data safeguard and reporting of the security breaches. Another concerns is The Regional and Country factors that impact on general stance towards the problem of information assurance. A culture on the national level defines the attitude of people in relation to protection, trust and risk [18]. For example, if such trust work and reliance is chiefly communal and hierarchal then it could involve exponentially more reliance on such small security sections of authority/leadership rather than the individualists. In contrast, the individualistic cultures that champion lacerative self-governance might provide more attention to detailing freedoms of the user rights and build the decentralized security frameworks with manifold distributed security responsibility to the user [19].

These disparities may cause tension to properly functioning multinational organizations, because organizations' hitherto, stakeholders and values, and hence their commitment to certain security measures may vastly differ due to cultural cognitive frames. For instance, what may be considered best practice in one country may seem different in another because of the difference in social culture, regarding issues to data privacy, surveillance or teamwork [20]. Therefore it can be said that organizations, which work on the global level, have to bear in mind these cultural distinctions when implementing IA solutions trying to make them as culturally sensitive and effective, as possible. Culture or culture in as a public also plays a role in information security. The result shows that using statistics data of societies having high privacy concern users may Sentry higher securities like using encryption services, using personal means of communication [21]. On the contrary, in societies where this aspect of privacy is not cherished highly people can freely offer their data thus expose



themselves to for instance fraudsters and other fraudulent personalities. These relative changes in the concerned collectivist perceptions about information security can alter the total risk by a huge margin [22].

Most of IA approach stems from the behavioral and culture perspectives and as IA as a discipline evolves all these aspects have to be acknowledged and incorporated into the central management of the policies and the stimuli that pertain to security. For example, in addition to offering commercial security services as well as securities products, organization should embark on organizational security culture transformation such as security sensitization, implementing security as a component of organizational work culture, organizational management / leadership development with appropriate security thinking [23]. Culture as an aspect under IA is one of the research sub components that have not undergone a call for either a revolutionary overhaul or its integration in the development of a perfect model for information assurance. It simply becomes possible that organizations are to deploy more of these relevant, more sensitive and more inclusive for protection of information when one just has an understanding of how these cultural phenomena that include organizational culture, national characteristics and societal culture are antecedents of behaviors and attitudes toward security. Focus on cultural elements of IA implies that security also deals with people and it means that security is not just needed on technical level, but is also in mission and vision statement of the organization [24].

INFORMATION RESOURCE MANAGEMENT: PROCEEDINGS OF THE ACADEMIC CONFERENCE

Social engineering is perhaps the most common type of threat and the most threatening one in the Information Assurance (IA) field As opposed to Technical threat in which one seeks to take advantage of the technology weakness of a certain system or communication network, someone takes advantage of the weakness of individuals to gain unauthorized access to a certain system, data or even a network that he or she should not be going near at all [25]. According to the paper's findings, the principal cause is that human factor are still the greatest threat to Information assurance as the social engineering involves deception categorized by psychological techniques that the attacker needs to appreciate while on the other hand, the defender does not. It can however be categorized as; phishing & pretexting spear phishing & baiting For instance, the activity that involves sending, actually, fake messages that are purporting to be from a particular source is called phishing. Their goal is to force the recipient to give something like a password, account information or anything looking like that [26]. Spear phishing is somewhat different in this regard because the attacker spends his or her time to focus on one single target or a firm, with the aim of establishing a rapport with the target and using the details of a social networking site account of the target. Even more challenging to identify and designed to be even more nefarious simply because they exploit all the basic safeguards and because they operate under the veil of the target's confidence [27].

Marketing resource managment USD-Billion 2023-2028

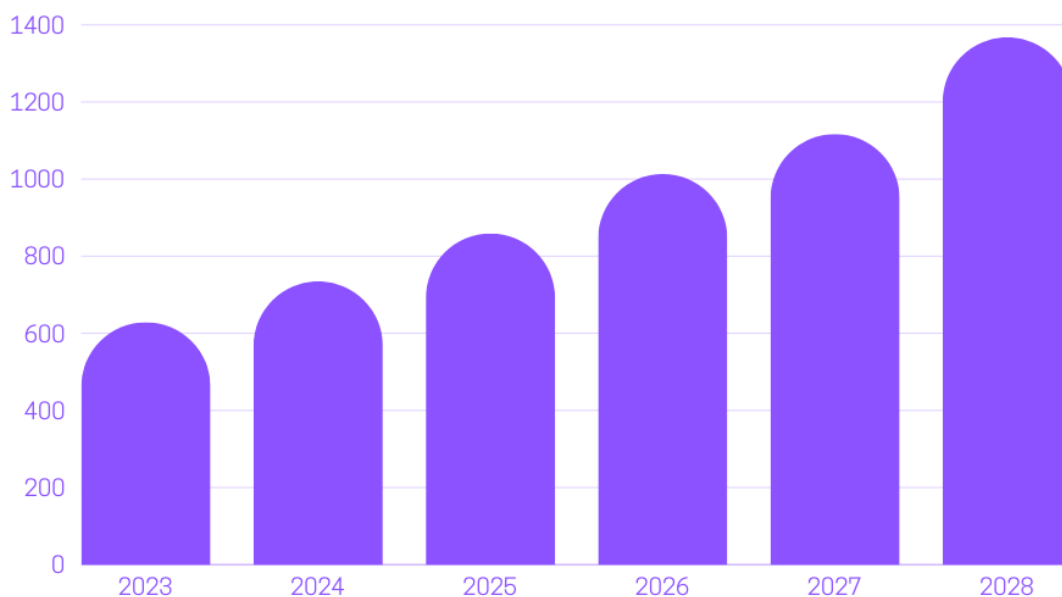


Figure: 3 showing marketing resource management

Another type of social engineering is so-called fake appointmenting, where an attacker will create some type of situation with the goal of making the target or victim reveal information. For instance, an attacker may camouflage as a technical person just to deceive an employee to provide him/her with the login credentials to carry out an update of the software





[28]. Similarly, baiting is a trick used in which the attacker offers the victim most probably wanted items in exchange for some personal details, clicking on an already known malicious program or link. That kind of strategies is built upon the untruth, and generally concern curiosity and sexual desire in a person – a reaction, which most people won't be able to restrain [29]. With this in mind, the major strengths of social engineering are psychosocial such as trust, fear, and sense of urgency or greed. For instance, whenever the content of the message is sensitive such as; the message tells the person that the account is sensitive for instance it has been reported that the bank account is sensitive, or your account will be suspended soon the individual will have to act without sparing time to think whether the sender of the message is real or fake. Similarly, the threat actors leverage extortive messages containing promises from authoritative purported individuals or entities, the target agrees to provide the details and perform other tricks as directed by the attacker [30].

As such, the psychological attack of a person with maneuvers, social engineering is one of the most complicated things to counter using only the IT environment. Hence, an effort to regulate the risks of social engineering is not as simple once and can be solved using tools that are confined to the domain of cybersecurity. This can extent to spearing people and users in the organizations informing them that they are being hit most through social engineering and providing information on things that these people can look at any odd emails and just discard [31]. It's also important that awareness training not only explain one case like when the employee received the letter from the attacker, or was called on the phone, but also let an employee know what information one should be cautious to deal with. To Alsea, organizations can combat social engineering attacks and their effects in the following ways, for example, MFA or even login details might have been hacked as well. They are: Strengthening and building up of policy and procedures; Changing and strengthening policies and guidelines; The phishing emails and demonstration emails; Building of reporting practices for social engineering threats and risks [32].

This kind of social engineering is one of the most efficient and threatening types of risks to information security, is based on human behavior and psychophysiological features. Since technology based protections remain necessary and sufficient for the protection of the ICT systems, it becomes mandatory that these gaps are complemented by a sufficient human security processes including training, awareness creation and organizational culture [33]. This shows that in general there are knowledge about techniques and methods of the SE attack in organizations, the possibilities of an organization being targeted by SE ... faktore mit mehr als 50% senken können. Some points that have been urged concerning IA with regard to social engineering are as follows: This needs stress on the technical treatment and also the behavioral standpoint to which one significant aspect of centrality for protection of such information belongs to [34].

IMPLEMENTING MEASURES AND INDIVIDUALS' CONDUCT IN THE SPHERE OF SECURITY

Security compliance also has a part to play in the plan of Information Assurance (IA) because it provides a blueprint of the legal and policy measures available to organizations and the kind of environment they need to provide for secure information. Still, in all these cases, compliance is not activated and steered exclusively with the assistance of technologies or by appeal to a reference frame; people and their work define compliance as a process [35]. Despite present Acts, regulation and individual security policies to prevent the breaches, these happens through human errors, negligence or noncompliance of the existing policies. I think it is necessary to evaluate some initial behavioral indicators related with compliancy and construct a new strategy to protect information and enhance the employees' safety degree. With regards to some of the objectives of a security compliance, some of the difficulties are that security requirement and security work do not correlate with organization's policy [36]. Much as people may know the security policies down to the last letter, it is when people do not see anything in common between the policies and one's job or when one is annoyed by the securities policy. For instance, change of passwords as often, or the use of multiple factors of authentication for instance, where the former feel that the latter is time-consuming or cumbersome since those workers work under a lot of pressure or are tied to tight schedules. Here we have the situation where overriding is traded for usability thus providing a real life proof that people action reduces security requirements [37].

Other behavioral factor which affects compliance is absence of awareness or total forgetfulness of the result of noncompliance. Some of the employees may not be very much aware of the outcome of their negligence to the security measures include; there is a possibility of being attacked by hackers, legal repercussions or else the company image is dragged in the mud [38]. Most of the time, such ignorance results from lack of practice or a wrong manner in which to explain issue concerning security policies. Since there is hardly any way that one can understand why or how some of these protocols may be required, then security becomes an extra fringe activity of an organization amongst its workers. This behavior is often supported by culture that was expected or told to be pro-business especially in open and flexible or result oriented culture. It also has to do with compliance/management of culture in an organization [39]. As a measure of Activism, it should however be pointed out that when the leadership proclaims security as an organizational necessity and strives to gain formal acknowledgement of compliance as a part and parcel of organizational culture, the employees will abide by the Security Standards. On the other hand if the management does not show its support and get the top management to recognize the problems that concern security then the employees would consider security as a raw deal [40]. Also, if the compliance concept is taken in its narrow or more technical form as a compliance check-list, of reference or bureaucratic process for the organization shield or defense, then employees will have their attention focused away from security, and may avoid doing what is needed towards compliance with the rules [41].

Besides, we could also gain understanding of the effect of compliance from the principles of behavioral economics. This





implies that the concept of nudge can be well appreciated from the premise that minor shift of how security policies is worded will compel adherence. For example it can be relatively easy to set higher standards for more rigorous compliance yet easier to follow for example password managers to create a new passwords with appropriate measures, it also wouldn't be difficult to make security sensitization for newly joining employees easier [42]. As such, the best that the organizations can do is to celebrate the positive behaviors and to make the process of compliance a little less painful for the employee. Also explained is that non-compliance has its advantages as well as disadvantages and vice versa. The activities that pertain to or concern the employees where such implications relate to or concern the security measures concerning the organization and positive or material returns are useful to an organization [43]. On the other hand, the negative consequences which need to be imposed; For cases where people are not following the security measures; demerits for cases of security violations, these are for people who are fond of violating security measures. But such measures must be taken gradually; That is, for the ad working of penalties – without making them punitive [44].

It also means that aspects concerning security requirements compliance are no longer a question of techniques, applications and solutions but also a question of regarding human activities. To ensure that such compliance is realized there is need for the organization to factor psychological variables on compliance and organizational culture as well as a comprehension of risks that contributed to noncompliance of the current security regulatory standards and policies and successful security policy that could improve on the security culture of an organization [45]. Organization promotion & training, commitment from the management & incentives/suggestion, informing the workers on the consequences of their non-compliance are useful in improvement of compliance by human aspect of organization security. Technical compliance controls coupled with the security awareness as suggested for people is ones of the slow and constant way of decreasing risks towards information security.

CONCLUSION

This may go well to state that IA is a combination of technical concepts and a managerial pertaining of the mind and the organizational unconscious. From time to time in this work it is clear that some of the behavioral and cultural aspects of IA should not be underplayed since humans are the cause of the security threats. What can be stated unquestionably is that no matter whether it is a question of cognitive biases and decision making emotional responses, or organizational culture of the incumbent company security practices, such sort of things seems to be beyond a doubt not fully avoidable in the course of constructing sustainable, efficient security frames. Insufficiently developed constructs of user security awareness, internal threats, desire for privacy and gain, inducing reckless action, and psychological predispositions are examples of how user behavior forms the concrete crack in technical security. Gathering the psychological incentives for users' behaviors must be considered as the further step toward better training models creation, awareness escalation, and development of easier and more effective security tools for the population that will entice compliance rather than saddle the latter. So too regarding those cultural factors – at both unit and country level – that has been found to shape attitudes towards security may well be useful for building context-sensitive cultures of security. The security concept is acceptable in an organization that has leadership commitment in addition to culture that enforces individual accountability for security.

Social engineering in IA also focuses on active IA as human vigilance since the attackers use psychological rather than technological techniques. Since deceptive attacks are categorized under social engineering, the problem can be eliminated by awareness and training, and by enrollment of preventive security measures such as using multiple factor authentication. While evaluating this view, the behavioral factors involved in the compliance with security show the possibilities of matching policy /management with other motivational theories such as motivational incentives, education and communication for the compliance of security. As a result, Information Assurance cannot be implemented while excluding technologies right at the time when human behaviors are characterized. It is not a project where the managers of information technology get to protect the data as it is a never-ending people, companies, and cultures involvement. Therefore, the IA needs human aspects of security where matters concerning people's attitude that supports or undermine security and organizational culture that is core to security in operating contexts of firms. Therefore, given that the sociology of information assurance has established that human psychology, organization culture and technology are the only social factors that predetermine the prospects of information assurance, to contemporary strategies need to be grounded on social experience in organizations.

REFERENCES

1. L. Atzori, A. Iera, G. Morabito, The Internet of things: a survey, *Comput. Netw.* 54 (15) (2010) 2787–2805.
2. B. Guo, D. Zhang, Z. Wang, Z. Yu, X. Zhou, and Opportunistic iot: exploring the harmonious interaction between human and the internet of things, *J. Netw. Comput. Appl.* 36 (6) (2013) 1531–1539
3. L. Yang, S.-H. Yang, L. Plotnick, How the internet of things technology enhances emergency response operations, *Technol. Forecast. Soc. Change* 80 (9) (2013) 1854–1867.
4. J. Wang, D. Rosca, W. Tepfenhart, A. Milewski, M. Stoute, Dynamic workflow modeling and analysis in incident command systems, *IEEE Trans. Syst. Man Cybern., Part A, Syst. Hum.* 38 (5) (2008) 1041–1055.
5. R. Nicolescu, M. Huth, P. Radanliev, D. De Roure, Mapping the values of iot, *J. Inf. Technol.* 33 (4) (2018) 345–360.





6. T. Floyd, M. Grieco, and E.F. Reid, Mining hospital data breach records: cyber threats to us hospitals, in: 2016 IEEE Conference on Intelligence and Security Informatics (ISI), IEEE, 2016, pp. 43–48.
7. E. Nakashima, Security firm finds link between china and anthem hack, Washington Post (2015).
8. Z. Qin, Y. Zhang, S. Meng, Z. Qin, K.-K.R. Choo, Imaging and fusing time series for wearable sensor-based human activity recognition, *Inf. Fusion* 53 (2020) 80–87.
9. O.-A. Kwabena, Z. Qin, T. Zhuang, Z. Qin, Mscryptonet: multi-scheme privacy-preserving deep learning in cloud computing, *IEEE Access* 7 (2019) 29344–29354.
10. Khan, M. I., Arif, A., & Khan, A. R. A. (2024). AI-Driven Threat Detection: A Brief Overview of AI Techniques in Cybersecurity. *BIN: Bulletin Of Informatics*, 2(2), 248-261.
11. Z. Qin, L. Hu, N. Zhang, D. Chen, K. Zhang, Z. Qin, K.-K.R. Choo, Learning-aided user identification using smartphone sensors for smart homes, *IEEE Int. Things J.* 6 (5) (2019) 7760–7772.
12. Z. Qin, Y. Wang, H. Cheng, Y. Zhou, Z. Sheng, V.C. Leung, Demographic information prediction: a portrait of smartphone application users, *IEEE Trans. Emerging Topics Comput.* 6 (3) (2016) 432–444.
13. D. Chen, N. Zhang, Z. Qin, X. Mao, Z. Qin, X. Shen, X.-Y. Li, S2m: a lightweight acoustic fingerprints-based wireless device authentication protocol, *IEEE Int. Things J.* 4 (1) (2016) 88–100.
14. H. Xiong, Y. Zhao, L. Peng, H. Zhang, K.-H. Yeh, partially policy-hidden attribute-based broadcast encryption with secure delegation in edge computing, *Future Gener. Comput. Syst.* 97 (2019) 453–461.
15. J. Sun, Y. Bao, X. Nie, H. Xiong, Attribute-hiding predicate encryption with equality test in cloud computing, *IEEE Access* 6 (2018) 31621–31629.
16. C. Xiao, D. Han, Y. Ma, Z. Qin, Csgan: robust channel state information-based activity recognition with gans, *IEEE Int. Things J.* 6 (6) (2019) 10191–10204.
17. Z. Qin, W. He, F. Deng, M. Li, Y. Liu Sprid, Pedestrian re-identification based on super-resolution images, *IEEE Access* 7 (2019) 152891–152899.
18. J.J. Gonzalez, A. Sawicka, A framework for human factors in information security, in: Wseas International Conference on Information Security, Rio de Janeiro, 2002, pp. 448–487.
19. Z. Qin, G. Huang, H. Xiong, Z. Qin, K.-K.R. Choo, A fuzzy authentication system based on neural network learning and extreme value statistics, *IEEE Trans. Fuzzy Syst.* (2019).
20. B. Schneier, *Schneier on Security*, John Wiley & Sons, 2009. [20] R. Klahr, J. Shah, P. Sheriffs, et al., *Cyber Security Breaches Survey 2017: Main Report*, 2017.
21. N.S. Safa, R. Von Solms, L. Fitcher, Human aspects of information security in organisations, *Comput. Fraud Secur.* 2016 (2) (2016) 15–18.
22. C.I. Canfield, B. Fischhoff, A. Davis, Quantifying phishing susceptibility for detection and behavior decisions, *Hum. Factors* 58 (8) (2016) 1158–1172.
23. M. Evans, Y. He, L. Maglaras, H. Janicke, and Heart-is: a novel technique for evaluating human error-related information security incidents, *Comput. Secur.* 80 (2019) 74–89.
24. D. Liginlal, I. Sim, L. Khansa, How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management, *Comput. Secur.* 28 (3–4) (2009) 215–228.
25. A.E. Speed, B.L. Woo, C.G. Kouhestani, J.J. Stubbs, G.C. Birch, Human factors in security, in: 2018 International Carnahan Conference on Security Technology (ICCST), IEEE, 2018, pp. 1–5.
26. Greig, A., Renaud, K. and Flowerday, S., 2015. An ethnographic study to assess the enactment of information security culture in a retail store. pp. 61–66.
27. Guldenmund F. The nature of safety culture: a review of theory and research. *Saf Sci* 2000;34(1–3):215–57. Available at: <http://www.sciencedirect.Com/science/article/pii/S092575350000014X>.
28. Habermas J. The theory of communicative action, vol 1: reason and the rationalization of society, Boston: Beacon Press; 1984. Translated by Thomas Mccarthy.
29. Hassan NH, Ismail Z. Information security culture in healthcare informatics: a preliminary investigation. *J Theor Appl Inf Technol* 2016; 88(2):202–9.
30. Helokunnas T, Kuusisto R. Information security culture in a value net. In: IEMC '03 Proceedings. Managing technologically driven organizations: the human side of innovation and change; 2003. p. 190–4.
31. Khan, M. I., Arif, A., & Khan, A. R. A. (2024). The Most Recent Advances and Uses of AI in Cybersecurity. *BULLET: Jurnal Multidisiplin Ilmu*, 3(4), 566-578.
32. Hofstede GH. Culture's consequences, 2nd ed: Comparing values, behaviors, institutions and organizations across nations. Thousand Oaks: Sage Publications, Inc; 2001. p. 924–31. Edn.
33. Alhogail A, Mirza A. Organizational information security culture assessment. In: International conference on security and management; 2015. p. 286–92.





34. Hughes-Morley A, et al. Factors affecting recruitment into depression trials: systematic review, meta-synthesis and conceptual framework. *J Affect Disord* 2015; 172:274–90.
35. Karlsson F, Astrom J, Karlsson M. Information security culture – state-of-the-art review between 2000 and 2013. *Inf Comput Security* 2015; 23(3):246–85.
36. Knapp KJ, et al. Information security: management’s effect on culture and policy. *Inf Manage Comput Security* 2006; 14(1):24–36.
37. Koh K, Ruighaver A, Maynard S, Ahmad A. Security governance : its impact on security Culture. In: *Proceedings of the third australian information security management conference*; 2005. p. 1–12.
38. Kolkowska, E., 2011. Security subcultures in an organization - exploring value conflicts.
39. Kraemer S, Carayon P. Computer and information security culture: findings from two studies. In: *Proceedings of the human factors and ergonomics society annual meeting*, 49; 2005. p. 1483–8.
40. Kuusisto R, Nyberg K, Virtanen T. Unite Security culture may a unified security culture be plausible? In: *Proc. of the 3rd European conference on information welfare and security*; 2004. p. 221–36
41. Liberati A, et al. The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: explanation and elaboration. *Ann Intern Med* 2009; 151(4):W65–94.
42. Lim JJS, et al. Embedding information security culture emerging concerns and challenges. In: *Pacis 2010*; 2010. p. 463–74.
43. Lim JS, et al. exploring the relationship between organizational culture and information security culture. In: *7th Australian information security management conference*; 2009. p. 88–97.
44. Lopes I, Oliveira P. Understanding information security culture: a survey in small and medium sized enterprises. *New Perspect Inf Syst* 2014; 1(275):277–86.
45. Mahfuth A, Yussof S, Baker A, Ali N. A systematic literature review: information security culture. In: *2017 International conference on research and innovation in information systems (ICRIIS)*; 2017. p. 1–6.

