Information Security: A Case of Clutter

Bineet Kumar Gupta[1], Abhishek Sachan[2], Rajnesh Kumar[3], Monika Gupta[4]

[1]Associate Professor, Faculty of CSE, Shri Ramswaroop Memorial University, UP India
bkguptacs@gmail.com
[2]Assistant Professor, Faculty of CSE, Shri Ramswaroop Memorial University, UP India
sachan.abhishek001@gmail.com
[3]Associate Professor, Faculty of MSS, Shri Ramswaroop Memorial University, UP India
rajnish.math@srmu.ac.in
[4]Assistant Teacher, PS Kursanda, Kasmanada, Sitapur, UP, India
monikagupta.upbe@gmail.com

Abstract: There is huge expansion in digital society during the last ten year. It is well obvious that number of applications contain security features which are presented for end-users to select and secure the potential to place users in situations where they must apply security related issues and decisions. However, it has also been noticed that the manner in which these aspects are implemented and presented can often serve to complicate the process to secure information such as users cannot actually use the security that they desire.

This paper presents the results of a survey of about 200 digital users in order to determine their consideration of the security features which they apply.

This study observes a new kind of prevailing problem named *InfoSec Sense Problem* among the digital users irrespective of age either teen age or younger or older at the same time irrespective of demographic or new user or expert user. Info Sec Sense problem is problem which is faced by digital users to manage multiple account. The study aims to observe reasons of digital user suffering from InfoSec Sense problem.

Keywords: *Information Security, Digital Society, Confidentiality, Security Threats, Risk*

1-Motivation: Information is an important asset. The more information you have at your command, the better you can adapt to the world around you. An obvious question which comes in mind is like what are you trying to protect, why are you trying to protect it? And how will you protect it? The serious success aspect in the modern world due to the growing distribution of information technologies within all areas of human society has enlarged their importance (Vance et al. 2012). Various kinds of damage resulting in significant economic losses, information processing systems are vulnerable to many different kinds of threats that can lead to unauthorized access, use, disclosure, disruption, modification, destruction. The insider malicious has the potential to cause more damage to the organization to target information directly and often to have knowledge of the organization and its processes and know the location of critical or valuable assets.

Outsiders need to target and gather many sources of intelligence as an external threat source to place to steal information rather than launch an attack through multiple layers of protection which can state to the extension and possible reduction of protection controls and access rights. This is a kind of making positive situation in topographical areas to allow new

opportunities for threat to identify information and vulnerabilities where individuals may be more susceptible to targeting and successful attack (Albrechtsen et al. 2009). Users are afraid of information systems misuse. One of the more concern towards information systems misuse means any insider behaviors that are deemed as a misuse of IS resources kept by the organization ranging from unethical and/or inappropriate uses to illegal uses of such behaviors (Egelman et al 2016: Hovav et al., 2012). Examples of IS misuse with the help of unlicensed software, and accessing confidential information, among others by company's email account to send network related jokes.

Fig 1: State of Various Security Approaches

Considering an information security culture in a digital society, researchers have to put attention towards the possibility of several information security subcultures that could be present in our daily routine work. There may be different traditions, values and opinions about the guarding of information depending upon different geographical, ethnic or age groups of users. It encourages towards in unique information security subcultures and need to understand how information security cultures and subcultures can be developed without having doubt over existing technologies (Mylonaset al. 2013).

1.1 Why Information Security:

There is a need of system to guide security implementations, responsible to focus on confidentiality, integrity, and availability of data. In the meantime there are several other models that focus on other aspects of

Fig 2 a: Common Threats to Digital User

Information security that is also important. Generally there are four components of security documentation are policies, standards, procedures, and guidelines. Together, these form the complete definition of a mature security program.

Data modification, mole, data theft, imitation and spoofing are the basic ad most common threats realized by digital user. Each user has sense to think of above before starting any electronic process over a network.

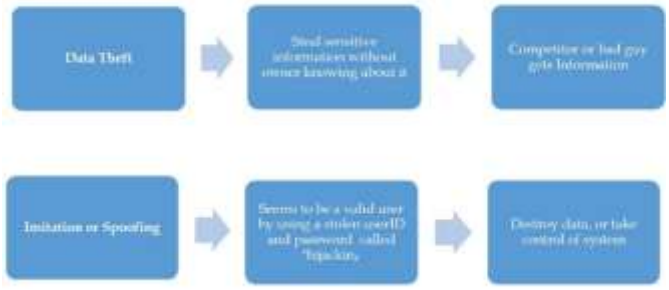

Fig 2 b: Common Threats to Digital User

1.2 Information Security Issue:

Awareness and adoption of information security focus on two aspects. The first one is extent to which user understands safe information security mechanism and which are often outlined in information security policies, rules and guidelines. The degree or extent to which every user applies in at the same time the levels of information security goes down as well as individual security responsibilities. The second aspect focuses on the behaviour in accordance with best practice like policies, rules and

guidelines (Parsons et al. 2017: Kruger and Kearney, 2006; Siponen, 2000).

Every time we cannot have expert user around our society and its quite obvious that he or she is not more aware about the confidentiality, integrity or availability which are the primary pillars of information security.

Fig 3: CIA Tried

The term data security is more popular among digital society and structured data looks like and where it resides to have tight control over who can access it. Sometimes the security controls are relatively cool steps to define and apply to structure data by applying either the built-in features of the structure or third-party tools designed for the particular structure (Furnell et al. 2016). It is much more difficult to manage and secure the unstructured data and unstructured data can live anywhere, in any format, and on any device, and can move across any network. Let us take an example of that many analysts say 80 percent or more of digital information in an organization is unstructured, and that the amount of unstructured data is obviously growing at a rate 10 to 20 times the rate of structured data.

Clearly it is prevailing for practical reasons, digital users have to secure the data within the database while also allowing legitimate users and applications to access it.

1.3 User's Perception about Security:

Data loss prevention (DLP) refers to a relatively new group of technologies designed for the process of monitor, discover, and protect data. It can be broken down into three types like Network DLP, Storage DLP and Endpoint DLP. Today's storage technologies can secure data natively by number of mechanisms; for example, many modern storage technologies include prefer to apply built-in encryption and automatic access control to protect confidentiality and integrity, redundancy to protect availability, and protection against malware (Jardine et al. 2015).

One of the causes to think about loss of security that 75% of digital users are heavily engaged in social engineering and at the same time there is risk to the security of information. Some of the most high profile cyber-attacks make smooth target of social engineering as an entry point into the organization's systems. Attackers use a number of tactics, ranging from simple impersonation to complex multilayered to disclose sensitive information. These attacks may be represented by a generic phishing email from an unknown sender that aims to misinterpret of information or lose online social networks (Calic et al. 2016: Scheelen et al. 2012).

Most of the digital users commonly maintains database as a part of processing and storage of information and to host many different databases and applications. Users have different types of permissions based on their job functions. Once a user has been allowed to connect to a server (through the use of a server login), the user will be given only the permissions that are granted to that login.

Different tools, such as social engineering, can been used to target individuals, who can be considered to be the weakest link of the security chain. Despite these high investments achieving higher information security, numerous software and hardware protection methods leads to security is low, significant information security risks do exist. It has become quite hard to maintain information smoothly in terms of gap of software and hardware and the number of security incidents does not decrease. The information security is only as robust as its weakest link no matter how many and how strong the layers of technological defenses in an organization (Miller et al. 2015). The weakest link of information security is to apply high degree of

mechanism to maintain and one with lack of consciousness Information Security are managed and operated by humans (Abawajy et al .2014: Guo et al. 2011))

2-Preliminary and Related Work:

Research shows that 70% of fraud is committed by insiders rather than by external criminals but that 90% of security controls and monitoring are focused on external threats (McCue, 2008). They must not be considered in isolation even where technical controls for insiders are available, (Jones and Colwill, 2008). With the suitable motivation and time, human presences will find their way. Around most technical controls greater investment in organizational human factors is required to balance against the funding in technology. Basic training and briefings can be used to measure actual behaviour in the workforce as part of organizational development for integrating security awareness and understanding culture of organization. In organisation third parties are now always present somewhere and may need to provide technical security results effective education for significant training in the form of computer based training (CBT) and onsite training personnel. In addition the organizational ethics are promoted and the way in which staff are trained and rewarded (Galba et al 2015: Colwill 2009).

It is well known accepted fact that security requirements cannot be addressed by technical means alone and for the purpose of chances of success will be significantly influenced by the people involved. As an example of the survey of IT abuse from the Audit Commission in the UK suggested that the majority of reasons that abuse is possible can be traced back to factors relating people of particular note was that more than a third cases were attributed to a lack of 'security awareness' (22%), or 'inadequate or insufficient training' (13%), evidencing that people need to know what is expected of them if they are to uphold security effectively.

The below study shows (Gizem et al. 2015: Furell et. Al. 2005) that the significant focus between

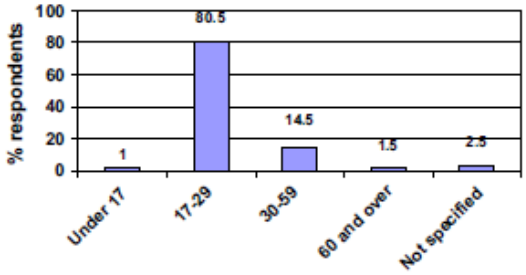

Fig 4: Age Profile of Respondent Group

17–29 category advocates that the most of opinion majority of opinions came from respondents who were easily involved in the upcoming technologies as part of their most of time. It is observed that 96.5% of the overall groups were involved as regular computer users at home and/or at work. The respondents also demonstrated a high level of achievement in more general education, with 82% claiming to hold a university level qualification.

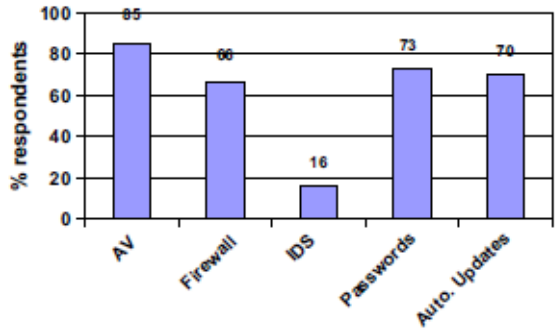

Fig 5: Use of Security Technologies

The amazing finding was that only three quarters of the respondents appealed to use passwords and a greater proportion having cause to use passwords in at least some scenario. A possible explanation for the lower result is that respondents were supposing that the question was related to use of passwords to protect their PC rather than in wider contexts.

Why users are about information security while using social media? A record-matching approach to the problem can be successful, with identifiers like last name, birth year and country while combining features can also prove effective

working with a wider range of features and design. Social media profiles allow for additional information to be exploited (Malhotra et al. 2012).

There are points to be noted down that social media profile information such as time stamps, geographical location and writing styles to match user profiles as well as users can still be identified based on their usage of the media. It demonstrates that even where usernames and other traditional identifiers are disguised,. The proposed method follows from this general design, using pictures, usernames, writing style, social graphs, content and location (Goga et al. 2013).

Experience of social engineering attack methodologies was asked to participants were asked to determine the real-world attack vectors used by social engineers, and understand their practicality for deployment and makes able to identify which techniques are more often used, and those that would be preferred. This included identifying the essential data needed to bootstrap an attack and which can still contribute to the effectiveness of an attack (Knowles et al. 2016).

Initially individuals' levels of awareness toward information security were examined in terms of both perception and behavioral aspect. Various security methods in terms of software and hardware are developed to make sure user that information can be kept secure. Information security risks cannot be removed completely by increasing information security awareness rather they can be minimized to a tolerable level. However, it is clearly seen that these methods are not sufficient between the individuals' awareness toward information security and their behaviors of using information and communication technologies within the scope of this study (Ogutcu et al. 2016).

3-Methodology:

A total of 200 digital users completed a questionnaire and participants were asked to meet the essential inclusion criteria. It was not necessary that users have to be degree qualified the essential element to participate in survey was whether do they use Internet or smart phones irrespective of geographical area. The age between 16 to 70 years and it is supposed that at least 20% of their work time is spent on computer or smart phones. , and work for an organisation with a formal or informal information security policy. At least they participants were familiar with the security of information and sensitive data.

Prior to data analysis, participants' responses were examined to evaluate data quality. We analyzed data based on content, which helps to identify responses with the same response option (e.g., "Strongly Agree") to all questions.

The designing of questions in the survey were based on the input from various researchers and experts of particular with the related studies in the account of the balances finally according to feedbacks and recommendations, the survey was redesigned with 13 questions for period of 2 months.

In terms of identifying digital divide the respondents were asked to identify whether they have digital accounts or not mainly it was 80% that have the digital accounts.

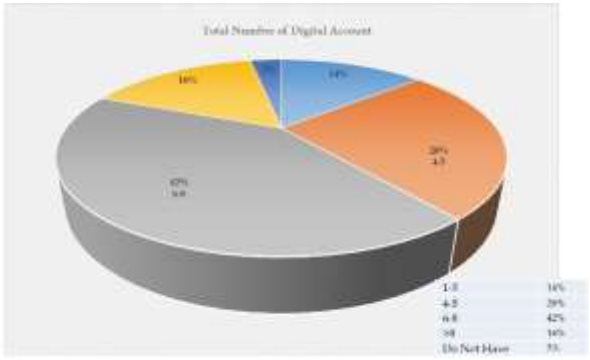

Fig 6: Total Number of Digital Account

Figure 6 represents that 42% respondents have digital account between six to eight and minimum number users not having digital account. It means most of the users are using familiar with transaction of information. This figure shows that digital society is increasing day by day and people are getting engaged with

online transfer of information either by using social media or by using other available options.

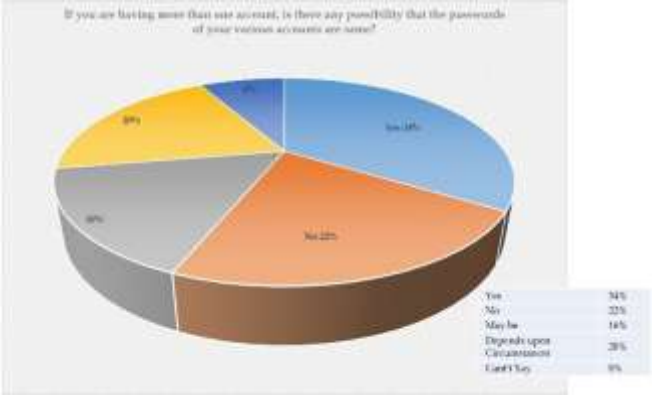

Fig 7: Password of Multiple Accounts

It is quite clear from above that most of the users have digital accounts between six to eight therefore they have to manage account in the form of passport. It is suggested that each account should have different password but surprising the result shows that 34% user keeps same password of multiple account. This is the higher rate of security threats in case anyone password is leaked by any on mechanism and resulting loss of information of other accounts. This is new kind of security threats which is generally not mentioned for information security.

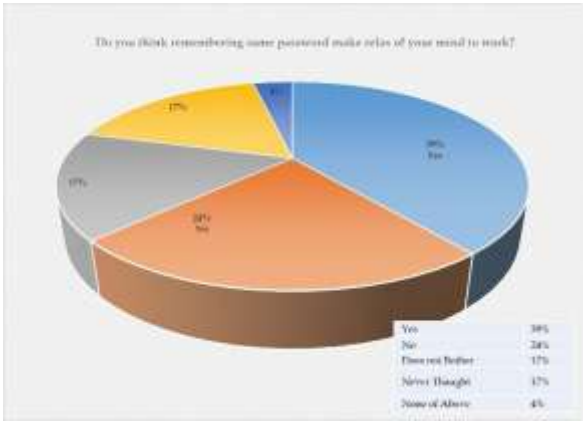

Fig 8: Why Same Password

This one of the important data that shows reason behind keeping same password of multiple accounts. 39% users answered that for relax of mind in form of ease of remember they keep same password of multiple accounts.24% responded that ease of remembering is not the reason. Hence we can say that just for the sake of relaxing mind people are keeping information on sensitive zones. More study can be done based on this data in future.

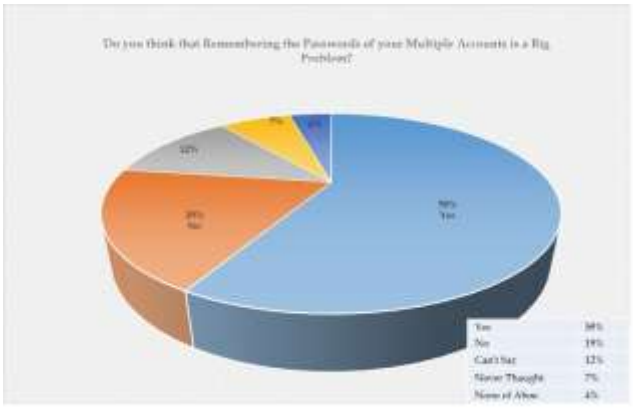

Fig 9: Is remembering Multiple Password Big Problem

This data is responsible to reveal the reason that why user keep same password of multiple accounts. The major data 58% shows that this problem is prevailing above half of the digital users. This is also notable that only 12% responded to not have problem of remembering password of digital accounts. This is one of the premier reasons which is responsible for loss of information and provides easy path for digital threats.

Due to the expanding speed of information and communication technology users have to work on multiple platform for online transaction of information or communication. Day by day process are becoming paperless and getting computerized. For this purpose digital users are compelled to create multiple accounts.

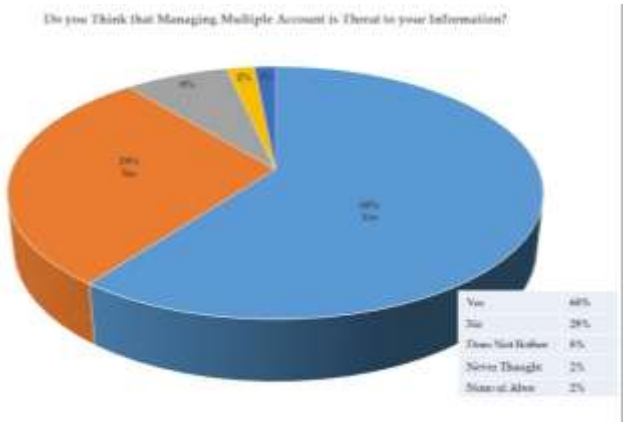

Fig 10: Managing Multiple Account

At the same time we can observe that digital users are getting stuck in digital process as it's very difficult to manage multiple accounts. About 60% of digital users accepted that is a kind of problem to manage multiple accounts. Hence we can say that it is a problem of inner layer. Means there is the risk of information security due to the multiple account moreover there is no chance of having less account due to the rapid growth of ICT

4-Conclusion:

There is huge expansion in digital society during the last ten year. It is well obvious that number of applications contain security features which are presented for end-users to select and secure the potential to place users in situations where they must apply security related issues and decisions.

The study reveals some significant areas of difficulty which is prevailing towards expert user as well. The standard security features presenting apparent usability challenges for large proportions of the respondents. The results state the need for a more considered approach towards the presentation of security functionality keeping in mind to reduce InfoSec Sense problem for better acceptability of security features if users have a realistic chance of protecting themselves.

- InfoSec Sense Problem exists among digital user irrespective of Age.
- It is responsible for to change the state of neuron in memory.
- Increasing information security features lead loss of information as well.
- However, it has also been noticed that the manner in which these aspects are implemented and presented can often serve to complicate the process to secure information such as users cannot actually use the security that they desire.

5-Result:

- The study reveals some significant areas of difficulty which is prevailing towards expert user as well.
- It shows that information security is a case of clutter and needs to be explored more deeply.
- The standard security features presenting apparent usability challenges for large proportions of the respondents.
- Result states that there is the need for a more considered approach towards the presentation of security functionality keeping in mind to reduce InfoSec Sense problem for better acceptability of security features.

There is the need to find out the transit state of neurons state between the state of neurons before applying security features and state of neuron after applying security features

6-Future Work:

There is big scope of presented study in the field of computing and neuro information.

- To identify parameters responsible to measure InfoSec Sense Problem
- An Algorithm to measure level of InfoSec Sense problem is supposed to be developed.
- As we apply different verify of security mechanism it lead more possibility of loss of information. Therefore a mechanism to prevent loss of information in this case while maintaining level of InfoSec Sense problem.
- Further to identify state of neuron during low level and high level of InfoSec Sense Problem.

7- Acknowledge:

I am very thankful to the Kalvi Institute of Theoretical Physics, University of California,

Santa Barbara-USA to provide a platform to discuss above ideas during the discussion session. Inputs received from eminent scientists brought a radical change in organizing this paper. I am thankful to the Director of KITP as well as Dr. Hynek (Director John Hopikan University) Dr. Richard and Dr. Malcoln (Google) respectively to encourage in this study.
Many more related ideas were adopted during the seminar, talks and discussion for future work in this field.
This paper was completed during my stay at KITP –UCSB in the program physics of hearing from Neurobiology to information theory and Back.
Finally the problem presented InfoSec Sense Problem leaves many more future researches like study of neuron states during different processes of applying information security and recovering information.

8-References:

1. Abawajy J. User preference of cyber security awareness delivery methods. Behav Inf Technol 2014;33(3):237–48.
2. Albrechtsen E, Hovden J. Improving information security awareness and behaviour through dialogue, participation and collective reflection: an intervention study. Computer and Security 2010;29:432–45.
3. Albrechtsen E, Hovden J. The information security digital divide between information security managers and users. Computers & Security 2009;28(6):476-90.
4. Arachchilage NAG, Love S. Security awareness of computer users: a phishing threat avoidance perspective. Comput Human Behav 2014;38(3) 4–12.
5. Baden R, Bender A, Spring N, Bhattacharjee B, Starin D. Persona: an online social network with user-defined privacy. Comput Commun Rev 2009;39(4):135–46.
6. Bechara A. Risky business: emotion, decision-making, and addiction. J Gambl Stud 2003;19(1):23–51.
7. Bertino E, Bonatti PA, Ferrari E. TRBAC: a temporal role-based access control model. ACM Transactions on Information and System Security (TISSEC) 2001;4:191-233.
8. Bertino E, Ferrari E, Atluri V. A flexible model supporting the specification and enforcement of role-based authorization in workflow management systems. In: RBAC'97: Proceedings of
9. Buchanan T, Paine C, Joinson AN, Reips UD. Development of measures of online privacy concern and protection for use on the Internet. J Am Soc Inf Sci Technol 2007;58(2):157–65.
10. Calic D, Pattinson M, Parsons K, Butavicius M, McCormac A. Naïve and accidental behaviours that compromise information security: what the experts think. In: Furnell SM, Clarke NL, editors. Proceedings of the 10th International Symposium on Human Aspects of Information Security and Assurance (HAISA 2016). Frankfurt, Germany: 2016.
11. Chen T, Kaafar MA, Friedman A, Boreli R. Is more always merrier?: a deep dive into online social footprints, in: Proceedings of the 2012 ACM Workshop on Online Social Networks,WOSN '12, ACM, NewYork, NY, USA, 2012, ,. 67–72.
12. D'Arcy J, Herath T. A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. European Journal of Information Systems 2011;20(6):643-58.
13. Davinson N, Sillence E. It won't han to me: promoting secure behaviour among Internet users. Comput Human Behav 2010;26(6):1739–47.
14. Edwards M,Wattam S, Rayson P, Rashid A. Sampling labelled profile data for

identity resolution, in: Proceedings of the IEEE International Conference on Big Data, IEEE, 2016.
15. Egelman S, Harbach M, Peer E. Behavior ever follows intention? A validation of the Security Behavior Intentions Scale (SeBIS). Paper presented at the Annual ACM Conference on Human Factors in Computing Systems, San Jose, CA, USA; 2016, 7–12.
16. Essmayr W, Probst S, Weippl E. Role-based access controls: status, dissemination, and prospects for generic security mechanisms. Electronic Commerce Research 2004;4:127-56.
17. European Union Agency for Network and Information Security (ENISA). The new users' guide: how to raise information security awareness (EN). 2010.
18. Ferraiolo DF. An argument for the role-based access control model. In: SACMAT'01: Proceedings of the 6th ACM Symposium on Access Control Models and Technologies. ACM
19. Fuchs L, Meier S. The role mining process model e underlining the need for a comprehensive research perspective. In: ARES'11: Proceedings of the 6th International Conference on Availability, Reliability and Security. IEEE Computer Society; 2011.
20. Furnell S, Clarke C. Power to the people? The evolving recognition of human aspects of security. Computer and Security 2012;31:9 83–89.
21. Galba T, Solic K, Lukic I. An Information Security and Privacy Self-Assessment (ISPSA) tool for internet users. Acta Polytech Hung 2015;12(7).
22. Gizem Ögütçü , Özlem Müge Testik, and Oumout Chouseinoglou "Analysis of personal information security behavior and awareness" computers & s e c u r i t y 2016: 56, 83–93.
23. Green B, Prince D, Busby J, Hutchison D. The impact of social engineering on industrial control system security, in: Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or Privacy, ACM, 2015, 23–9.
24. Guo KH, Yuan Y, Archer NP, Connelly CE. Understanding nonmalicious security violations in the workplace: a composite behavior model. Journal of Management Information Systems 2011;28(2):203-36.
25. Harrington SJ. The effects of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. Management Information Systems Quarterly 1996; 20(3):257-78.
26. Hoonaker P, Bornoe N, Carayon P. Password authentication from human factors perspective: results of survey among end users. In: Proceedings of Human Factors and Ergonomics
27. Horst M, Kuttschreuter M, Gutteling JM. Perceived usefulness, personal experiences, risk perception and trust as determinants of adoption of e-government services in The Netherlands. Comput Human Behav 2007;23(4):1838–52.
28. IBM Global Technology Services. IBM security services 2014 cyber security intelligence index. IBM Global Technology Services; 2014. 12-19
29. Ifinedo P. Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. Computers & Security 2012;31(1):83-95.
30. Im GP, Baskerville RL. A longitudinal study of information system threat categories: the enduring problem of

human error. The Data Base for Advances in Information Systems 2005;36(4): 68-79.
31. Jagatic TN, Johnson NA, Jakobsson M, Menczer F. Social phishing. Commun ACM 2007;50(10):94–100.
32. Jardine E. Global cyberspace is safer than you think: real trends in cybercrime. Global Commission on Internet Governance Paper Series No 16; 2015.
33. Joinson A, Reips U, Buchanan T, Schofield P. Privacy, trust and self disclosure online. Hum Comput Interact 2010;25:1–24.
34. Kathryn Parsons et al. "The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation stud" computers & s e c u r i t y 2017: 66 , 40–51.
35. Krombholz K, Hobel H, Huber M,Weippl E. Social engineering attacks on the knowledge worker, in: Proceedings of the 6th International Conference on Security of Information and Networks, ACM, 2013, 28–35.
36. Kruger H, Kearney W. A prototype for assessing information security awareness. Computer and Security 2006; 25(4):289–96.
37. Meade AW, Craig SD. Identifying careless responses in survey data. Psychol Methods 2012;17(3):437–55
38. Miller KW, Voas J, Hurlburt GF. BYOD: security and privacy considerations. IT Professional 2012;14(5):53–5.
39. Morrow B. BYOD security challenges: control and protect your most sensitive data. Netw Secur 2012;2012(12):5–8.
40. Mylonas A, Kastania A, Gritzalis D. Delegate the smartphone user? Security awareness in smartphone platforms. Computer and Security 2013;34:47–66.
41. Narayanan A, Shmatikov V. De-anonymizing social networks, in: Proceedings of the 30th IEEE Symposium on Security and Privacy (S&P 2009), IEEE Computer Society, 2009, 173–87.
42. Ng B-Y, Kankanhalli A, Xu Y. Studying users' computer security behavior: a health belief perspective. Decis Support Syst 2009;46(4):815–25.
43. Oh S, Sandhu R. A model for role administration using organization structure. In: SACMAT'02: Proceedings of the 7th ACM Symposium on Access Control Models and Technologies. ACM Press; 2002, 155-62.
44. Padayachee K. Taxonomy of compliant information security behavior. Computers & Security 2012;31(5):673-80.
45. Park J, Sandhu R. The UCON_ABC usage control model. ACM Transactions on Information and System Security (TISSEC) 2004;7:128-74.
46. Parsons K, McCormac A, Pattinson M, Butavicius M, Jerram C. The design of phishing studies: challenges for researchers. Computer and Security Spec Issue SEC 2013 Conf 2015a;52: 194–206.
47. Pattinson M, Butavicius M, Parsons K, McCormac A, Jerram C. Examining attitudes toward information security behaviour using mixed methods. In: Furnell S, Clarke N, editors. Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015). Mytilene, Greece: Centre for Security, Communications & Network Research; 2015b. p. 57–70.
48. Perito D, Castelluccia C, Kaafar MA, Manils P. How unique and traceable are usernames? In: Privacy Enhancing Technologies. Springer; 2011, 1–17.
49. Rainer RK Jr, Snyder CA, Carr HH. Risk analysis for information technology. J Manag Inf Syst 1991;8(1):129–47.
50. Rezgui Y, Marks A. Information security awareness in higher education: an

exploratory study. Computer and Security 2008;27:241– 53.
51. Sandhu R, Bhamidipati V. The ASCAA principles for nextgeneration role-based access control. In: ARES'08: Proceedings of the 3rd International Conference on Availability, Reliability and Security. 2008.
52. Scarfo A. New security perspectives around BYOD. In Proceedings of the 2012 Seventh International Conference on Broadband, Wireless Computing, Communication and Applications (446–451). IEEE Computer Society, 2012.
53. Schultz EE, Proctor RW, Lien M-C, Salvendy G. Usability and security an appraisal of usability issues in information security methods. Computer and Security 2001; 20(7):620–34.
54. Siponen M, Adam Mahmood M, Pahnila S. Employees' adherence to information security policies: an exploratory field study.Inf Manage 2014; 51(2):217–24.
55. Siponen MT. A conceptual foundation for organizational information security awareness. Inf Manage Computer and Security 2000; 8(1):31–41.
56. Society 53rd Annual Meeting. 2009.
57. Son JY. Out of fear or desire? Toward a better understanding of employees'
65. American Society for Information Science and Technology 2006; 58(2):212-22.

motivation to follow IS security policies. Inf Manage 2011;48(7):296–302.
58. Stewart G, Lacey D. Death by a thousand facts: criticising the technocratic approach to information security awareness. Inf Manage Computer and Security 2012;20(1):29–38.
59. the 2nd ACM Workshop on Role-based Access Control. ACM Press; 1997, 1-12.
60. Trcˇek D, Trobec R, Pavešic´ N, Tasicˇ JF. Information systems security and human behaviour. Behav Inf Technol 2007;26(2):113–18.
61. Vance A, Siponen M, Pahnila S. Motivating IS security compliance: insights from habit and protection motivation theory. Inf Manage 2012; 49(3–4):190–8.
62. von Solms B, von Solms R. The 10 deadly sins of information security management. Computer and Security 2004;23(5):371–6.
63. Whitman ME. In defense of the realm: understanding the threats to information security. International Journal of Information Management 2004;24:43-57.
64. Workman M, Gathegi J. Punishment and ethics deterrents: a study of insider security contravention. Journal of the