Human mistakes in the information security realm and solutions

Nader Sohrabi Safa[a], Carsten Maple[b]
Cyber Security Centre at WMG, University of Warwick, Coventry, United Kingdom[a,b]
Email: n.sohrabisafa@gmail.com[a], CM@warwick.ac.uk [b]

Abstract

Information security breaches and privacy violations are major concerns of many organizations. Human behaviour, either intentionally or through negligence, is a great potential of risk to information assets. It is acknowledged that technology alone cannot guarantee a secure environment for information assets; human considerations should be taken into account as well as technological and procedural aspects. This article strives to present a useful classification of users' mistakes in the domain of information security. The outputs of this study shed some light for both academics and practitioners.

Introduction

It is well-understood that an information security breach can have serious consequences for an organization. Losing reputation, competitive advantage, funds, future revenue, productivity, intellectual property and in the worst scenario bankruptcy are some results of information security breaches. For example, the defence industry has usually several suppliers; they share information among each other to increase productivity. Information security leakage in such a sector can have serious impacts on national security. For these reasons, considering all aspects that can mitigate the risk of information security breaches is necessary. A remarkable portion of these threats relates to the human mistakes. Sharing password and user name with colleague, writing login information on a sticky paper and putting on monitor or desk, using social number as password, using simple password without special characters (dictionary words), downloading software from the Internet, carrying organizational data in external hard or pen drive, leaving systems logged-in while in unattendance, opening unknown email and its attachments, changing password through the email (phishing) and so forth are simple examples of employees' mistakes. Users' negligence, ignorance, lack of awareness, mischievousness, apathy and resistance are usually the reasons for information security breaches (Sohrabi Safa, Von Solms et al., 2016).

In addition, bribery, embezzlement, espionage and sabotage are the other reasons of many information security breaches. Previous studies have shown that anger, fear of losing a job, revenge, joy and even entertainment are psychological roots of some information security breaches (Posey, Bennett et al., 2011). Table 1 classifies the reasons for users' mistakes in the domain of information security in a concise form.

Table 1: Classification of users' misbehaviour

Type of mistakes	Reasons
Intentionally	Gaining benefit
	Getting revenge
	Anger
	Fear of losing job
	Joy and entertainment
	Bribery
	Embezzlement
	Espionage
	Sabotage
	Resistance
Unintentionally	Apathy
	Ignorance
	Lack of awareness
	Mischievous
	Negligence

Unauthorised extraction, exfiltration, differentiation, duplication are actions that threat confidentiality, integrity and availability of information by employees. As can be seen, information security management cannot be effective and efficient unless human aspects of information security are taken into consideration comprehensively.

The lack of awareness

Awareness is a key element in information security assurance. Suitable information security training is necessary to improve users' awareness. Formal presentations, games, Internet pages, email, meetings, posters, pens and screen savers are key methods to improve individuals' knowledge and awareness (Safa, Sookhak et al., 2015). Hackers use creative, ingenious and novel methods to achieve their targets. They abuse the lack of awareness in users to advance their agenda. Ignorance is the primary reason for many information security breaches. Risks and threats change frequently and as such the information security training programmes should be updated regularly. To keep employees updated, an awareness program should be an integral part of organizational culture (Abawajy, 2014). Consistent and relevant plans are the key to success in information security awareness. Information security awareness and keeping up date about the methods that attackers may use, play important role to mitigate the risk of information security breaches. Information security knowledge sharing, collaboration, intervention (different training methods) heighten the level of awareness (Safa and Von Solms, 2016).

Social engineering

Social engineering refers to psychological manipulation of individuals into performing actions to disclose confidential information. Indeed, social engineering focuses on human mistakes. Social engineering encompasses a variety of methods to deceive people into divulging their private information. The most general type of social engineering occurs over the phone. Another example of this threat is criminals posing as exterminators, fire marshal and technicians to go unnoticed as they steal company secrets. In another case, an individual who walks into a building and posts an official-looking announcement to the organization building that says the number of helpdesk has changed; when staff call for help the offenders ask them for their password and other information in order to access private organizational information. Social networks also have a great potential for violation of privacy; offenders contact the target slowly and gently, start to conversation to create a trust. Then use it to get information about bank account details and password. The ability of hackers in social engineering and the lack of awareness in victims are two important factors in this kind of crime (Safa, Solms et al., 2016).

Misleading software

Attackers are frequently seeking to find new approaches to distribute malware. Misleading software is a novel method that they use recently. A fake Anti-Virus (AV) represents an active trend for malware distribution. Attackers disguise malware as legitimate AV software and seduce individuals to install it. Many of people are not aware of this kind of traps (Kim, Yan et al., 2015). Web browsers have been become the most popular applications for many of users to find online resources, Internet pages are the dominating tool to lunch fake AV attacks. Misleading software also can show a fake bad sector on your hard disk and ask you to install suggested software to repair your hard disk. The internet is a huge environment with a great potential of novel and creative methods to hack your systems. Knowledge and understanding of how to recognise and deal with misleading software (for example through reporting mechanisms) through a suitable training programme can keep users updated about such threats. Figure 1 shows the source of information security threats that are associated to human behaviour.

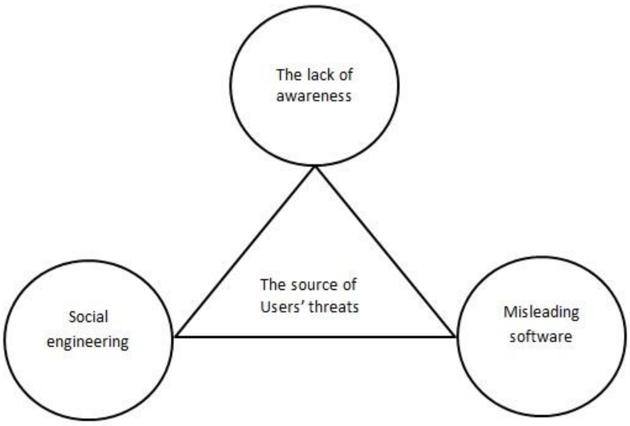

Figure 1: Users' information security threats

Solutions

The aforementioned threats focus on human behaviour. Information security awareness plays a vital role in avoiding such mistakes. Effective and efficient approaches are presented in the following sections that mitigate the risk of human behaviour in the domain of information security.

Conscious care behaviour

Conscious care behaviour means that users think about the consequences of their actions in terms of information security when they work with a system, particularly on the Internet. Conscious care behaviour is an effective approach to counter creative attacks to reduce the risk of information security breaches (Safa et al., 2015). When a user is faced with a suspicious email that asks him/her to change his/her username or password, user awareness and knowledge about phishing sends the first alarm to his/her mind. The user starts to think about the consequences of changing the username and password through the email. Based on organizational information security policy, employees should not reply to this kind of email, because any change of username and password should be conducted through the official procedure. Individuals' awareness, knowledge, experience, and involvement in information security have been mentioned as important factors that affect conscious care behaviour.

Complaining with organizational policies

The Internet is a huge environment with a great variety of information security threats. It is acknowledged that complying with organizational information security policies and procedures is important due to diversity of threats that have surrounded employees. Information security policy can prompt employees to consult with experts before any action in a suspicious situation, such as phishing, social engineering and misleading software. Information security policies and procedures should be clear and easy to understand (Kirlappos, Parkin et al., 2015). These policies should be updated frequently due to the dynamic nature of the threats (Ifinedo, 2014). Attachment to organization, commitment to organizational aims and plans, involvement in information security activities and personal norms that complying with organizational information security policies and procedures is important, influence employees' decision about complying with organizational information security policies and procedures. In this regards, involvement can be in the form of information security collaboration, knowledge sharing and training courses (Sohrabi Safa et al., 2016).

Information security knowledge sharing

Knowledge sharing plays an important role in the domain of information security, due to its positive effect on employees' information security awareness. Knowledge sharing is particularly useful in combatting phishing, social engineering and impact of misleading software such as fake anti-virus and disk repairing software.It is acknowledged that security awareness is the most important factor that mitigates the risk of information security breaches in organizations.

Experts face similar problems in this domain and they should provide proper solutions for them. Preventing the development of the same solutions for similar problems by way of sharing knowledge leads to the avoidance of time-wasting and extra costs (Feledi, Fenz et al., 2013). This time and funding could be better spent by improving the quality of solutions, instead of reinventing the security wheel. However, previous study has shown that the motivation for knowledge sharing among employees is a challenge in this realm. Sharing previous relevant experiences in the domain of information security is a valuable resource in information security awareness. Previous research showed that extrinsic motivation, such as earning reputation and gaining promotion, and intrinsic motivation, such as curiosity satisfaction and self-worth satisfaction, can significantly influence individuals' attitude to share their information security knowledge in organizations (Safa and Von Solms, 2016).

Information security collaboration

Collaboration is working together to do or achieve a common goal. One such goal could be the protection of information assets in organizations. Collaboration is a major subject in diverse research and disparate fields such as learning, project management, organization, health, business and so forth. Collaboration reduces the cost, improves ability to pursue goals, increases benefits through sharing expertise and improves decision making and innovation through sharing ideas. Knowledge sharing, learning, improvement of productivity and performance are further advantages of inter-organizational collaboration. Collaboration also increases the chance of problem solving.

Information Security Collaboration (ISC) aims to aggregate employees' contribution against information security breaches. Information security collaboration has been acknowledged as an effective and efficient approach to mitigate the risk of information security incidents (von Solms and von Solms, 2004). Shared goals, benefit, personal interest, organizational support are examples of factors that motivate individuals to collaborate.

Poor commitments, communication, trust, coordination, culture of collaboration, supervision besides concentration on technical skills rather than collaboration are barriers to collaboration. Previous studies have shown that weak collaboration causes vulnerabilities to information in distributed, inter-dependent, and collaborative environments (Werlinger, Hawkey et al., 2009). To perform a security task, employees should corporate, coordinate and collaborate with others. These interactions are distinguished by the level of commitment and intensity of the relationship. Responsibility means sharing our knowledge and experience with each other and realising that we must work together to have secure environment. Capturing, integrating, submitting, commenting, reviewing and sharing our information security knowledge are samples of collaboration.

Figure 2 shows how employees can mitigate information security breaches in organizations.

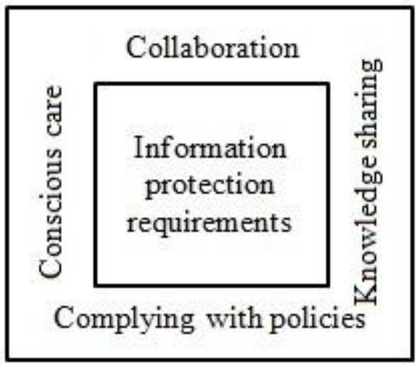

Figure 2: Information security requirements in organizations

Closing statement

This article endeavours to present an overview of human errors in the domain of information security in a concise form. In addition, we have described some solutions that other experts have presented previously to mitigate the risk of aforementioned mistakes. We believe that these issues can provide pointers for further academic research and for managers to have a more secure environment for information assets.

References

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour and Information Technology, 33*(3), 236-247. doi: 10.1080/0144929X.2012.708787

Feledi, D., Fenz, S., & Lechner, L. (2013). Toward web-based information security knowledge sharing. *Information Security Technical Report, 17*(4), 199-209. doi: http://dx.doi.org/10.1016/j.istr.2013.03.004

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management, 51*(1), 69-79. doi: http://dx.doi.org/10.1016/j.im.2013.10.001

Kim, D. W., Yan, P., & Zhang, J. (2015). Detecting fake anti-virus software distribution webpages. *Computers & Security, 49*(0), 95-106. doi: http://dx.doi.org/10.1016/j.cose.2014.11.008

Kirlappos, I., Parkin, S., & Sasse, M. A. (2015). "Shadow security" as a tool for the learning organization. *SIGCAS Comput. Soc., 45*(1), 29-37. doi: 10.1145/2738210.2738216

Posey, C., Bennett, R. J., & Roberts, T. L. (2011). Understanding the mindset of the abusive insider: An examination of insiders' causal reasoning following internal security changes. *Computers & Security, 30*(6–7), 486-497. doi: http://dx.doi.org/10.1016/j.cose.2011.05.002

Safa, N. S., Solms, R. v., & Futcher, L. (2016). Human aspects of information security in organisations. *Computer Fraud & Security, 2016*(2), 15-18. doi: http://dx.doi.org/10.1016/S1361-3723(16)30017-3

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security, 53*(0), 65-78. doi: http://dx.doi.org/10.1016/j.cose.2015.05.012

Safa, N. S., & Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior, 57*, 442-451. doi: http://dx.doi.org/10.1016/j.chb.2015.12.037

Sohrabi Safa, N., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security, 56*, 70-82. doi: http://dx.doi.org/10.1016/j.cose.2015.10.006

von Solms, B., & von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security, 23*(5), 371-376. doi: http://dx.doi.org/10.1016/j.cose.2004.05.002

Werlinger, R., Hawkey, K., Botta, D., & Beznosov, K. (2009). Security practitioners in context: Their activities and interactions with other stakeholders within organizations. *International Journal of Human-Computer Studies, 67*(7), 584-606. doi: http://dx.doi.org/10.1016/j.ijhcs.2009.03.002