WHAT DO WE KNOW ABOUT THREATS FROM WELL-INTENTIONED USERS, A LITERATURE REVIEW

Natalia Derbentseva, Brenda Fraser, Sarah Gibbon and Andrea Hawton

Defence Research and Development Canada, 1133 Sheppard Ave. W., Toronto, Ontario M3K 2C9 Canada

Abstract: *We surveyed open academic and practitioner information security literature on non-malicious user threat behaviours with the purpose of 1) identifying possible non-malicious user threat behaviours; 2) understanding the reasons for these behaviours and 3) identifying mitigation strategies to minimise non-malicious user threat behaviours proposed in the literature. This paper presents a summary of our findings.*

Key words: *Human factors of cyber security, non-malicious behaviour, policy non-compliance*

For a long time information security was seen predominantly as a technical issue, and the field focused on the development of technical solutions to the security problems. However, experts soon recognised that technical solutions alone could not protect an organization's information systems (IS) from breach and compromise [1]. "It does not matter how many firewalls, encryption software, certificates, or two-factor authentication mechanisms an organization has if the person behind the keyboard falls for phish" (p. 74, [2]). People are an integral part of the information security equation. Systems exist for people and every system has a user. People use the systems to achieve their organizational and individual goals; however, not everyone who has legitimate access to these systems is well versed in the most recent information security threats and protection mechanisms, or they may not even be fully aware of their organization's Information Systems Security Policies (ISSP). Sophisticated attackers are becoming increasingly skilled at tricking unsuspecting users into to allowing them access to the systems [3, 4].

Some information security scholars argue that the majority of information security breaches happen as a result of internal incidents [5], and they view the internal staff as the most significant threat to information security [6]. Humans in general have been dubbed the weakest link of information security [3], and this paper examines what it is that we, humans, do that gave us this reputation.

This paper reports on the results of an open literature survey, the primary goal of which was to identify user behaviours that could potentially lead to an IS incident or vulnerability, and the causes of these behaviours. The focus of this paper is on *non-malicious* insider behaviour, i.e., behaviours by legitimate system users that do not have intent to cause harm to the organization or its IS. In other words, we examine the ordinary user behaviour that poses risk to organization's IS. Thus, our analysis includes *accidental errors* in Im and Baskerville's taxonomy [7], but excludes

deliberate threats as they all have an underlying malicious motive. From Stanton et al. taxonomy [8], *dangerous tinkering* and *naïve mistakes* fall within the scope of our analysis, but not *intentional destruction* and *detrimental misuse.* From Guo's taxonomy [9], we consider *security risk-taking behaviour,* but exclude *security damaging behaviour* as Guo attributes malicious intent to this category.

Also, our analysis mainly focuses on threat behaviours in *organizations*, as opposed to users' private (personal) computing practices; although we realise that this distinction has become somewhat blurred with the current teleworking practices and widespread use of social media in all aspects of people's activities, including professional [10, 11].

Our open literature search began with a Web of Science topic search using keywords "user" or "user behaviour" combined with "information security" or "cyber security." The results returned over 100 papers. These papers were evaluated based on their relevance to the focus of this work, i.e., non-malicious user behaviour that can pose a threat to information systems. The initial review of the most relevant papers was followed by a cited reference search, which allowed us to identify and locate other relevant papers referenced in the initial sample. The current review is based on over 80 journal articles, and it is by no means exhaustive or comprehensive. In this paper we summarise the main trends in the literature regarding non-malicious user threat behaviours, proposed explanations for these behaviours, and mitigation strategies that have been suggested or tested.

The papers we reviewed used a variety of methodological approaches, including tests with unsuspecting users (e.g., [12-14]), controlled experiments (e.g., [15-17]) surveys (e.g., [18-20]), interviews (e.g., [20-24]), focus groups (e.g., [25, 26]); training workshops (e.g., [27, 28]), game-based training (e.g., [29, 30]) and system dynamics modelling (e.g., [31]).

One of the main purposes of this review was to create a catalog of possible user threat behaviours that could potentially lead to an IS incident, but that do not have an underlying malicious intent. From the papers reviewed, we identified over 40 such threat behaviours, which we grouped into ten general thematic categories. Table 1 reports the categories of user threat behaviours with examples of specific actions that contributed to each category, and some references that either mentioned or explicitly studied these user actions.

All of the threat behaviours in Table 1 are the result of either user *actions* or *inactions*, which could be *intentional* or *unintentional* [9, 32-34]. Focusing on intentionality may be helpful in understanding potential underlying causes of the behaviours. For example, using action intentionality, Reason [32] differentiates human errors into three general categories: 1) *slips/lapses* happen when an unexpected outcome results from an unintended action or inaction, e.g., accidentally clicking on a send button instead of a save button in an unfinished e-mail message window; 2) *mistakes* happen when an unexpected outcome results from an intended action, e.g., a user not recognising a well-crafted phishing e-mail, believing that it

came from a colleague and opens an attachment; and 3) *violations* are instances of deliberate disobedience of the rules, e.g., deciding not to scan a USB memory key before plugging it into the system while the policy, of which the user is aware, states that all external media must be scanned.

Table 1: Categories and examples of user threat behaviours.

#	Category	Examples of specific actions	References
1	Internet use, browsing	Careless web browsing visiting unsafe webpages; downloading files from unverified sources.	[2, 28, 29, 35]
2	E-mail practices	Opening e-mails from unknown sources; falling prey to phishing e-mails – clicking on embedded links or opening attachments.	[12, 36-38]
3	Password practices	Generating weak passwords, reusing passwords on multiple platforms and accounts, writing down passwords.	[8, 39-41]
4	Account protection	Not locking workstation when away from it, being logged in and allowing others to use workstation or sharing account details.	[19, 35, 41, 42]
5	Removable media	Failure to scan media, using unauthorised media, failure to encrypt data on media.	[9, 19, 43, 44]
6	Work – home blur	Sending business e-mails or files to personal e-mail address; connecting to an unknown network while working outside of organization (e.g., a coffee shop)	[9, 20]
7	Use of Social media	Revealing too much information on social media; posting undesirable information.	[10, 11, 45]
8	Use of personal devices in the workplace	Connecting personal devices to organization's systems or network, storing work files on personal devices.	[9, 43]
9	System maintenance	Failure to update the operating system or antivirus protection in a timely manner; not backing up data regularly; ignoring security warnings or changing security settings.	[44, 46, 47]
10	ISSP non-compliance	Not following information systems security policies (ISSP) or not reporting ISSP breaches	[9, 20]

Slips and *lapses* can have numerous underlying causes, but most often result from distraction of attention or memory faults. These actions are not intended and likely will not be repeated again, at least not on purpose. It is impossible to completely mitigate or eliminate slips and lapses, as they are inherent to human nature [32, 34]. However, their occurrence may be reduced through user-centered design of systems' interfaces, memory and attention aids, and associated organizational procedures [34].

Slips and lapses occur relatively frequently and could contribute to security incidents [32, 34, 48], however mistakes and violations have often been found to be associated with more serious accidents [48] and thus they deserve more in-depth analysis.

Mistakes happen when a user executes the planned action correctly, i.e., she does exactly what she wanted to do; however, the action leads to a different outcome from what she intended. Norman [34] and Reason [32] describe mistakes as a failure at the planning stage of action. Examples of mistakes in the IS security context mainly originate from users not fully understanding or not recognising the threats [16, 49, 50], or not being aware of, or not fully understanding proper policies and procedures, [50-53]. For example, a user might plug her phone into a USB port on her station just to recharge the phone's battery. The user does not see this action as a violation of the policy prohibiting plugging unauthorised USBs into the organization's systems, because in her mind she is using the USB port on her system only as a charger and not to transfer files between the two devices. The user does not realise that data exchange takes place between the phone and the system as soon as the phone is plugged in, and that the system (or the phone) might get infected with malware as a result, without any deliberate user-initiated copying of files from one to the other. This particular behaviour could be classified as a violation from the policy standpoint, however from the user's perspective it is rather a mistake, because the user did not intend to violate the policy.

People's vulnerability to social engineering attacks and their inability to recognise deception can lead to mistakes as well [17, 54, 55]. One of the most widespread social engineering practices is phishing attacks that trick unsuspecting users into responding to malicious e-mails or interacting with fraudulent websites [17, 24, 28, 36, 55, 56]. According to the Canadian Cyber Incident Response Centre (CCIRC), phishing attacks have been the second most prevalent incident type handled by CCIRC, accounting for about 30% of all the incidents handled by this organization during the past year [57].

Falling for phishing has been attributed to a combination of factors, including lack of threat awareness [28, 36]; general human propensity to trust [24, 54]; manipulation of emotional triggers such as fear, greed or sexual interests [2]; peripheral processing of the message that could result from many factors including but are not limited to distractions, urgency, workload, overall e-mail load [56, 58], habitual media use [56], as well as individual characteristics such as information security self-efficacy [56], age or gender [55]. Spear phishing attacks, which are individually crafted and more successful (with reported success rates from 30% to over 50% [55, 58, 59]), have been rising in volume [2, 14, 58] and pose a significant risk to organizations. Social engineering risks to IS security are not limited to e-mail or website phishing attacks. Social engineering has been successfully used to gain access to systems without the aid of these mechanisms [54].

While it might be impossible to eliminate human mistakes entirely, increasing user awareness as well as providing education and training on topics such as security, threats, reasons behind security policies, and how to better detect phishing have the potential to significantly reduce the number of mistakes that occur in the workplace [2, 28, 30, 55, 59-61]. Unfortunately, many existing security awareness, education and training programs are often ineffective due to their delivery style, infrequency, mandatory nature and lack of user engagement. Further work is required to make these programs more effective [28, 30, 58, 62].

Violations are intentional breaches of ISSPs, however in this paper we are concerned only with *non-malicious violations*. Non-malicious violations, as we define them, do not have an underlying malicious intent to harm the organization, and violators do not intend the negative outcomes of their actions. Policy violations are not unique to information security; they have been studied for quite some time by the safety community in different domains [32, 48].

While the information security literature does not always agree on the reasons for ISSP violations, there seems to be agreement among scholars that ISSP violations are fairly common in the workplace [43, 48, 63, 64]. There is also a consensus that there is a cost to security, and that security procedures require extra effort on the part of users [35, 39, 65], which goes against the human instinct to strive to minimize the effort used to complete their tasks [35, 66].

Often the blame for poor security practices falls on the users, because it is the users who violate ISSPs. There has been some discussion regarding users' motivation for ISSP violation [42, 64, 67-69]. One line of thinking views users as rational actors who engage in cost-benefit analysis of their anticipated actions and they choose those behaviours that maximize their expected outcome. Based on this rational choice view of user behaviour, the General Deterrence Theory (GDT) has been one of the widely used theories in IT security literature [70], which suggests that users need monitoring and external stimuli to ensure compliance [71]. The main premise of GDT is that presence of certain and severe sanctions (external stimuli) for ISSP violations will deter users from violating the policies [70, 72].

While the evidence is mixed regarding the effectiveness of the GDT-based approach [42, 51, 64, 67, 68, 72, 73], its main limitation, in our view, is the emphasis on the extrinsic motivational factors that are only effective while they are present and do not result in sustainable changes in human behaviour once they are removed. In addition, Hedstrom et al. [69] argue that internal value systems have a more profound impact on people's decisions to obey or violate policies, and that people choose those behaviours that are in line with their moral beliefs even if it may lead to sanctions and reprimand.

A somewhat different view on user motivation for not complying with ISSPs is based on understanding that the additional workload that ISSPs require of the user adds to their existing workload and strains users' limited resources which creates inconvenience, delay, and hampers users' productivity [20, 35, 39, 65, 74]. Quite

often, ensuring security is a secondary task for most users who are primarily concerned with getting their job done well and on time. Given that in many user communities productivity is valued more than security, and productivity (not security!) is what the users are evaluated on and rewarded for, it is not surprising that they often choose productivity over security [20]. The bottom line is that users find themselves faced with a "productivity – security" conflict and often have to choose one or the other [20, 22].

When ISSPs interfere with the immediate user's tasks, users find themselves in a situation where they cannot follow the policies [1, 75]. This creates another conflict – users who consider themselves "good employees" feel that they are forced to engage in security-undermining, or, simply put, "bad" behaviour. This conflict creates cognitive dissonance, which is uncomfortable and motivates people to take measures to reduce it [76]. Literature suggests that users may take a somewhat "active" approach to reducing this conflict by inventing their own security practices [22] or they may employ purely cognitive mechanisms to reduce it [43, 73].

Kirlapos et al. [22] found that users try to reduce potential risk from their actions by following their own "do-it-yourself" security procedures and do the best they can to protect the organization's resources, short of following the official policy. The user-invented "shadow" security practices are based on users' understanding of threats and adequate protection mechanisms, and this understanding might be incomplete or erroneous [22]. These actions although not ideal, allow users to reduce cognitive dissonance that might result from policy violation.

Another approach to reducing the uncomfortable feeling resulting from policy violation is to employ various cognitive neutralisation strategies [43, 73]. Siponen and Vance [73] discuss six such strategies and report empirical support for their effectiveness in predicting users' intent to violate ISSPs. According to Siponen and Vance [73] users can engage in the following cognitive rationalizations of their actions: 1) the violation was beyond the user's control; 2) the violation did not cause any harm; 3) the user had no choice; 4) the ISSP is unreasonable, therefore it is okay to violate it; 5) the user's job completion was in jeopardy; 6) an occasional violation is okay (in light of their generally good behaviour).

All of these strategies help the user to reduce the perceived significance and negativity associated with their ISSP violation and therefore to reduce their internal conflict. Recognising the danger of these cognitive mechanisms in contributing to ISSP violations, Barlow et al. [43] found that neutralization-discouraging communication was as effective in reducing users' intent to violate ISSP as GDT-based communication about sanctions. However, the Barlow et al. [43] approach emphasised the unacceptability of justifying one's violation of ISSPs without educating users further on the risks to which their actions expose the organization. Thus, their approach can be extended to include user education to enhance user understanding of the threat environment and technological self-efficacy [18, 44].

Often, ISSP violations do not result in negative outcomes and pass unnoticed, especially if they are socially accepted within the organization, which may further reinforce the unsafe practices. In addition to reducing cognitive dissonance, the lack of negative feedback may alter user's risk perception, reinforcing the overly optimistic assessment of the threat environment. Perceived risk is a major motivator for user ISSP compliance [77]; however, people are prone to underestimate their own risk and vulnerability. This phenomenon, frequently referred to as optimistic bias, extends to the cyber domain as well [78]. Rhee et al. [78] recommend implementing systematic user awareness programs to reduce the undue cyber risk optimism among managers and users.

While examining the state of existing security mechanisms and policies, some scholars argue that the nature of ISSPs and security mechanisms that users are required to use contribute a great deal to whether users comply with the policies or not [74]. For example, usability of security mechanisms, such as authentication tools and procedures [1, 74, 79], and policy usability, i.e., whether the users understand what the policy requires them to do and whether they are able to do it [50-52], have a significant impact on their behaviour. For example, many authentication policies require users to remember multiple long and random passwords, which is not feasible given the properties of human memory, rendering such policies unusable [1, 75, 80].

Similarly, user perception of policy legitimacy, i.e., whether the users view a given policy as an appropriate (effective) and justifiable measure to protect against the threat, has an impact on their compliance [42]. One can argue that perceived ISSP legitimacy is closely related to users' threat awareness [49, 50], because if users do not understand the threat from which the policy is trying to protect the organization, then it is difficult for them to understand the reason for the policy and, thus, they will be less likely to comply [81].

In addition, users' beliefs is their own skills and ability to comply with the policy, i.e., their self-efficacy, also has a significant impact on their ISSP compliance [18, 44, 82]. Therefore, policy usability is a complex concept and compliance is dependent on the characteristics of the specific audience for which it is designed.

The organization of the work environment plays a significant role in ISSP compliance [23, 25, 83-85]. While conducting interviews with security specialists, Kraemer and Carayon [23] found that organizational factors such as culture, structure, policy and communication were the most frequently mentioned elements contributing to information security human error and ISSP violations. Employees' organizational commitment, or their attachment to the organization, has also been shown to influence their intent to comply with ISSPs [86].

Management in the organization plays an important role not only in ISSP compliance enforcement, but also in influencing employees' attitudes towards security, security policies and forming an overall organizational security culture [83-85, 87]. Organizational culture, defined as shared assumptions, beliefs and social norms within an organization, has a profound impact on employee behaviour [88],

including their information security behaviour and ISSP compliance [25, 85, 87]. For example, if a work team develops a norm of password sharing within the team to ensure timely response to clients' needs, then it will be very difficult for a new team member not to follow this norm even if it goes against an official policy.

The above is just a brief summary of some of the most notable factors contributing to non-malicious human information security jeopardising behaviours, and it is by no means an exhaustive list. Some of these factors apply to specific issues, such as the fact that properties of human memory have a profound impact on user's password behaviour. Other factors are more general and can lead to a variety of issues, for example an organizational culture that is focused on productivity and disregards security, which may encourage general ISSP non-compliance and contribute to a whole range of user threat behaviours including password practices, external media use, use of personal devices and handling work documents outside of the workplace.

A number of approaches have been proposed in the literature to help mitigate some of these issues. There have been efforts made to develop technological solutions that silently eliminate the threat and require no user action. While there are benefits to these solutions, it has been argued that these technological approaches are not entirely flawless [28], and given that these are not the focus of our work they will not be covered here. Below we discuss three main approaches to mitigating user threat behaviour – usable security approach; motivational approach; and user security education, training and awareness approach.

The *Usable security* approach, instead of blaming the user for mistakes and ISSP violations, focuses on the interaction between the user and various security mechanisms and procedures that they have to use or follow [22, 75, 89]. The goal of this approach is to improve the usability of these mechanisms and procedures by taking users' cognitive characteristics, tasks and needs into account. This includes designing security mechanisms that do not add extra workload to the users; including the security considerations at the forefront of system design instead of adding them as an afterthought; giving due consideration to the user tasks; identifying causes of undesirable user behaviour and addressing them by improving usability of security measures; and involving end users in policy design [1, 21, 22, 65].

According to the usable security approach, effective ISSP design relies on user involvement in order to understand and account for the causes of these violations and to develop effective solutions [1]. The success of this approach often depends on the ability of the users to report security violations to the policy designers without the fear of consequences, which might be easier said than done in an organizational context.

While the usable security approach has a potential to mitigate all types of user threat behaviours including slips, lapses, mistakes and violations, the *motivational approach* focuses on ISSP violations. The goal of the motivational approach is to understand the motivation behind user behaviour with the ultimate goal of altering it in the desired direction. Both extrinsic motivators, such as sanctions, penalties [70,

72] and social pressure [64] and intrinsic motivators, such as professional values [69], value congruence with the organization [42], and perceived contribution [64], have been considered and supported in the literature. Many of the studies investigating motivational factors focused on the users' intent to comply (or violate) policies as opposed to the actual compliance. While some authors argue that both intrinsic and extrinsic motivations could be effective in influencing users' behaviour [64], others argue that intrinsic motivation provides a more powerful explanation [42].

Moreover, extrinsic factors rely on such organizational measures as continuous user monitoring, objective administration of sanctions, and the development of an internal culture conducive to creating adequate social pressure to comply. Employing intrinsic motivational factors on the other hand, may require deeper understanding of the user community and their values, and they may also require amendments to the policy and user education campaigns that emphasise value congruence.

What we can learn from the studies on user motivation in ISSP compliance is that both extrinsic and intrinsic motivational factors may play a role in shaping user ISSP compliance intentions. However, it remains unclear what conditions make each of these sets of factors more or less effective.

The last, and probably the most important, mitigation approach that we would like to discuss is *user security education, training and awareness*, or SETA for short [90, 91]. Users are a vital link in the cyber security chain, and their actions depend to a large extent on their perception of threats, and their assessment of the situation. Studies have shown that when users see the need for implementing security measures they are motivated to do so [39]. The ability to do this in turn depends on users' understanding of the threats and potential consequences, protection mechanisms, organizational policies, and their options for mitigating the threats. Users' understanding of security risks is fundamental to information security [81] and SETA has been a constantly recurring theme in our review.

User training and education not only motivates the need for security and teaches the necessary skills [28], but it can also influence and develop a desirable organizational culture [88] and improve users' technological self-efficacy [44], all of which have been shown to influence user ISSP compliance.

However, many SETA programs have been found to be ineffective [91, 92]. Possible reasons for these programs' ineffectiveness could be unsuitable delivery methods; failure to establish a connection between pertinent user problems and learning material; natural learning decay and a lack of refreshers; failure to adjust the work environment to allow for the new behaviours to set in; lack of users' practical experience; and lack of users' motivation to learn about security. A number of different training approaches that apply instructional principles from learning science [28] and attempt to remedy some of the above issues have been proposed, including participative workshops [27] and hands-on interactive games [28-30], . Some studies provide evidence that more participative and experiential training and education

programs are more effective than the traditional top-down approaches [12, 27] and that follow up reminders and refreshers reinforce learning [93].

As our brief review demonstrates, the contribution of human factors to cyber security is a multifaceted problem, and there is an abundance of factors that can contribute to user information security threat behaviours. It is important to recognise that user behaviours that jeopardise security take place in a given organizational context, while the user is performing a certain task and trying to achieve a certain goal. In line with Kraemer and Carayon's macroergonomic framework [23], it is helpful to view the resulting user behaviour as a function of multiple interdependent factors including the individual characteristics of the user, task properties and demands, properties of the technology that is being used and the organizational environment in which the behaviour takes place. Therefore, addressing user threat behaviours also requires a multidimensional approach including greater user involvement in security mechanisms and policy design, continuous security education, training and awareness programs and examination of organizational factors, including the incentive structure, values and culture.

References

1. Sasse, M.A., S. Brostoff, and D. Weirich. Transforming the 'weakest link' — A Human/Computer Interaction Approach to Usable and Effective Security. BT Technology Journal 2001, 19(3), 10.
2. Hong, J. The State of Phishing Attacks. In *Communications of the ACM.* New York, NY, USA: ACM, 2012, vol. 55, p. 8.
3. Schneier, B. *Secrets and lies: digital security in a networked world*. Edtion ed.: Wiley, 2000.
4. Schneier, B. Phishing has gotten very good. In., 2013, vol. 2015.
5. Nash, K.S. and D. Greenwood. The global state of information security. In *CIO Magazine.* 2008, vol. 22 (3).
6. Williams, P.A.H. In a 'Trusting' Environment, Everyone is Responsible for Information Security. Information Security Technical Report, 2008, 13(4), 9.
7. Im, G.P. and R.L. Baskerville. A Longitudinal Study of Information System Threat Categories: The Enduring Problem of Human Error. The Database for Advances in Information Systems, 2005, 36(4), 12.
8. Stanton, J.M., et al. Analysis of End User Security Behaviors Computers & Security, 2005, 24(2), 10.
9. Guo, K.H. Security-Related Behavior in Using Information Systems in the Workplace: A Review and Synthesis. Computers & Security, 2013, 32, 10.
10. Phillips, K.N., A. Pickett, and S. Garfinkel. Embedded with Facebook DoD Faces Risks from Social Media. In D.o. Defense. Cross Talk, 2011, vol. May/June, p. 6.

11. Molok, N.N.A., S. Chang, and A. Ahmad. Disclosure of Organizational Information on Social Media: Perspectives from Security Managers. In *Pacific Asia Conference on Information Systems (PACIS)*. Jeju Island, Korea, 2013.
12. Bowen, B.M., R. Devarajan, and S. Stolfo. Measuring the Human Factor of Cyber Security Homeland Security Affairs, 2012, Supplement 5(Article 2).
13. Dodge Jr, R.C., C. Carver, and F.A. J. Phishing for User Security Awareness. Computers & Security, 2007, 26, 8.
14. Jagatic, T., et al. Social Phishing. Communications of the ACM, 2007, 50(10), 94-100.
15. Parsons, K., et al. 2013. Phishing For The Truth A Scenario-based Experiment Of Users Behavioural Response To Emails. In *Proceedings of the Security and privacy protection in information processing systems: 28th IFIP TC 11 International Conference, SEC 2013, Auckland, New Zealand, July 8-10, 2013*, July 8-10, 2013 2013, L. Janczewski, H.B. Wolfe, and S. Shenoi eds. IFIP TC11 International Conference on Information Security.
16. Liu, D., X. Wang, and L.J. Camp. Mitigating Inadvertent Insider Threats with Incentives. In *Financial Cryptography and Data Security Conference*. Springer Berlin, 2009, p. 1-16
17. Alsharnouby, M., F. Alaca, and S. Chiasson. Why phishing still works: User strategies for combating phishing attacks. International Journal of Human-Computer Studies, 2015, 82, 69-82.
18. Bulgurcu, B., H. Cavusoglu, and I. Benbasat. Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. MIS Quarterly, 2010, 34(3), 33.
19. Siponen, M. and A. Vance. IS Security Policy Violations: A Rational Choice Perspective. Journal of Organizational and End User Computing, 2012, 24(1), 24.
20. Kirlappos, I., A. Beautement, and M.A. Sasse. "Comply or Die" Is Dead: Long Live Security-Aware Principal Agents. In A. Adams, M. Brenner, and M. Smith eds. *Financial Cryptography and Data Security*. Springer Berlin Heidelberg, 2013, vol. 7862, p. 70-82.
21. Kirlappos, I. and M.A. Sasse. What Usable Security Really Means: Trusting and Engaging Users. In T. Tryfonas and I. Askoxylakis eds. *Human Aspects of Information Security, Privacy, and Trust*. Springer International Publishing, 2014, vol. 8533, p. 69-78.
22. Kirlappos, I., S. Parkin, and M.A. Sasse. Learning from "Shadow Security:" Why understanding non-compliant behaviors provides the basis for effective security. 2014.
23. Kraemer, S. and P. Carayon. Human Errors and Violations in Computer and Information Security: The Viewpoint of Network Administrators and Security Specialists. Applied Ergonomics, 2007, 38, 12.
24. Wright, R., et al. Where Did They Go Right? Understanding the Deception in Phishing Communications. Group Decision and Negotiation, 2009, 19(4), 26.
25. Kraemer, S., P. Carayon, and J. Clem. Human and Organizational Factors in Computer and Information Security: Pathways to Vulnerabilities. Computers & Security, 2009, 28(7), 12.

26. Kumaraguru, P. PhishGuru: A System for Educating Users about Semantic Attacks. Carnegie Mellon University, 2009.
27. Albrechtsen, E. and J. Hovden. Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. Computers & Security, 2010, 29, 14.
28. Kumaraguru, P., et al. Teaching Johnny Not to Fall for Phish. ACM Transactions on Internet Technology, 2010, 10(2), 31.
29. Abawajy, J. User preference of cyber security awareness delivery methods. Behaviour & Information Technology, 2012.
30. Cone, B.D., et al. A Video Game for Cyber Security Training and Awareness. Computers & Security, 2007, 26, 10.
31. Dutta, A. and R. Roy. Dynamics of Organizational Information Security. System Dynamics Review, 2008, 24(3), 27.
32. Reason, J. *Human Error*. Edtion ed. New York, NY: Cambridge University Press, 1990.
33. Norman, D. Design rules based on analyses of human error. Communications of the ACM, 1983, 26(4), 254-258.
34. Norman, D. *The design of everyday things*. Edtion ed. New York: Basic Books, 1988.
35. Albrechtsen, E. A qualitative study of users' view on information security. Computers & Security, 2007, 26, 14.
36. Wang, J., et al. Phishing Susceptibility: An Investigation Into the Processing of a Targeted Spear Phishing Email. IEEE Transactions on Professional Communication, 2012, 55(4), 18.
37. Aytes, K. and T. Connolly. Computer Security and Risky Computing Practices: A Rational Choice Perspective. Journal of Organizational and End User Computing, 2004, 16(3), 19.
38. Kearney, W.D. and H.A. Kruger. Phishing and Organisational Learning. In L.J. Janczewski, H.B. Wolf, and S. Shenoi eds. *SEC 2013*. IFIP International Federation for Information Processing, 2013, vol. IFIP AICT 405, p. 379-390.
39. Adams, A. and M.A. Sasse. Users are not the Enemy. Communications of the ACM, 1999, 42(12), 40-46.
40. Florencio, D., C. Herley, and P.C. van Oorschot. 2014. Password Portfolios and the Finite-Effort User: Sustainably Managing Large Numbers of Accounts. In *Proceedings of the 23rd USENIX Security Symposium*, San Diego, CA, USA, August 2014 2014.
41. Tam, L., M. Glassman, and M. Vandenwauver. The Psychology of Password Management: A Tradeoff between Security and Convenience. Behaviour & Information Technology, 2010, 29(3), 13.
42. Son, J.-Y. Out of Fear or Desire? Toward a Better Understanding of Employees' Motivation to Follow IS Security Policies. Information & Management, 2011, 48, 7.
43. Barlow, J.B., et al. Don't make excuses! Discouraging neutralization to reduce IT policy violation. Computers & Security, 2013, in Press.

44. Rhee, H.-S., C. Kim, and Y.U. Ryu. Self-Efficacy in Information Security: Its Influence on End Users' Information Security Practice Behavior. Computers & Security, 2009, 28, 11.
45. Lenkart, J.J. The Vulnerability of Social Networking Media and the Insider Threat: New Eyes for Bad Guys. Naval Postgraduate School, 2011.
46. Liang, H. and Y. Xue. Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective. Journal of the Association for Information Systems, July 2010 2010, 11(7), 21.
47. Besnard, D. and B. Arief. Computer Security Impaired by Legitimate Users. Computers & Security, 2004, 23, 16.
48. Matthews, G., et al. *Human performance: Cognition, stress and individual differences*. Edtion ed. Hove, UK: Psychology Press, 2000.
49. Cen, C.C., R.S. Shaw, and S.C. Yang. Mitigating information security risks by increasing user security awareness: A case study of an information security awareness system. Information Technology, Learning, and Performance Journal, 2006, 24(1), 1-14.
50. Dinev, T. and Q. Hu. The centrality of awareness in the formation of user behavioral technologies. Journal of the Association for Information Systems, 2007, 8(7), 386-408.
51. D'Arcy, J., A. Hovav, and D. Galletta. User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. Information Systems Research, Articles in Advance, 2008, 20.
52. Al-Omari, A., O. El-Gayar, and A. Deokar. Security Policy Compliance: User Acceptance Perspective. In *International Conference on System Sciences.* Hawaii, 2012.
53. Knapp, K.J. and C.J. Ferrante. Policy Awareness, Enforcement and Maintenance: Critical to Information Security Effectiveness in Organizations. Journal of Management Policy and Practice, 2012, 13(5), 16.
54. Conheady, S. *Social engineering in IT security: Tools, tactics, and techniques*. Edtion ed. Toronto: McGraw-Hill Education, 2014.
55. Sheng, S., et al. 2010. Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions. In *Proceedings of the CHI 2010: Privacy Behaviors* Atlanta, GA, April 10-15 2010.
56. Vishwanath, A., et al. Why do People get Phished? Testing Individual Differences in Phishing Vulnerability within an Integrated, Information Processing Model. Decision Support Systems, 2011, 51(3), 11.
57. CCIRC Quarterly cyber operations report. In P.S. Canada. 2014-2015.
58. Caputo, D.D., et al. Going spear phishing: Exploring Embeded Training and Awareness. IEEE Security & Privacy, 2014, 12(1), 28-38.
59. Kumaraguru, P., et al. 2007. Getting Users to Pay Attention to Anti-Phishing Education: Evaluation of Retention and Transfer. In *Proceedings of the APWG eCrime Researchers Summit*, Pittsburgh, PA, USA., October, 4-5, 2007 2007.
60. Kumaraguru, P., et al. School of Phish: A Real-World Evaluation of Anti-Phishing Training. In *Proceedings of the 5th Symposium on Usable Privacy and Security.* Mountain View, California: ACM, 2009, p. 1-12.

61. Sasse, A., et al. Human Vulnerabilities in Security Systems. C.S.K.T. Network, 2007.
62. Zhang-Kennedy, L., S. Chiasson, and R. Biddle. Password Advice Shouldn't Be Boring: Visualizing Password Guessing Attacks 2013.
63. Willison, R. and M. Warkentin. Beyond Deterrence: An Expanded View of Employee Computer Abuse. MIS Quarterly, 2013, 37(1), 21.
64. Herath, T. and H.R. Rao. Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness. Decision Support Systems, 2009, 47, 12.
65. Beautement, A., A. Sasse, and M. Wonham. 2008. The compliance budget: Managing security behaviour in organizations. In *Proceedings of the New Security Paradigms Workshop*2008 ACM, New York, NY, 47-58.
66. Zipf, G.K. *Human behavior and the principle of least effort; an introduction to human ecology*. Edtion ed. New York: Hafner, 1972.
67. Pahnila, S., M. Siponen, and A. Mahmood. 2007. Which Factors Explain Employees' Adherence to Information Security Policies? An Empirical Study. In *Proceedings of the Pacific Asia Conference on Information Systems (PACIS)*2007.
68. Liang, H., Y. Xue, and L. Wu. Ensuring Employees' IT Compliance: Carrot or Stick? Information Systems Research, Articles in Advance, 2013, 16.
69. Hedström, K., et al. Value Conflicts for Information Security Management. Journal of Strategic Information Systems, 2011, 20, 12.
70. D'Arcy, J. and T. Herath. A Review and Analysis of Deterrence Theory in the IS Security Literature: Making Sense of the Disparate Findings. European Joumal of Information Systems, 2011, 20, 16.
71. Hu, Q., et al. Does Deterrence Work in Reducing Information Security Policy Abuse by Employees? Communications of the ACM, 2011, 54(6), 7.
72. D'Arcy, J. and S. Devaraj. Employee Misuse of Information Technology Resources: Testing a Contemporary Deterrence Model. Decision Sciences Journal, 2012, 43(6), 34.
73. Siponen, M. and A. Vance. Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. MIS Quarterly, 2010, 34(3), 29.
74. Sasse, M.A., et al. The Great Authentication Fatigue – And How to Overcome It. In P.L.P. Rau ed. *Cross-Cultural Design.* Springer International Publishing, 2014, vol. 8528, p. 228-239.
75. Angela Sasse, M. Technology Should Be Smarter Than This!": A Vision for Overcoming the Great Authentication Fatigue. In W. Jonker and M. Petković eds. *Secure Data Management.* Springer International Publishing, 2014, p. 33-36.
76. Festinger, L. *A theory of cognitive dissonance*. Edtion ed. Stanford: Stanford University Press, 1962, c 1957.
77. Ostowan, B. Towards a framework to measure user compliance with computer security practices. Stockholm University, 2006.
78. Rhee, H.-S., Y.U. Ryu, and C.-T. Kim. Unrealistic Optimism on Information Security Management. Computers & Security, 2012, 31, 12.

79. Chiasson, S., P.C. van Oorschot, and R. Biddle. 2006. A Usability Study and Critique of Two Password Managers. In *Proceedings of the 15th USENIX Security Symposium*, Vancouver, Canada2006.
80. Forget, A., S. Chiasson, and R. Biddle. Supporting Learning of an Unfamiliar Authentication Scheme. In *Association for the Advancement of Computing in Education AACE E-LEARN*. Montreal, Canada, 2012.
81. Spears, J.L. and H. Barki. User Participation in Information Systems Security Risk Management. MIS Quarterly, 2010, 34(3), 503-522.
82. 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, 13.
83. Knapp, K.J., et al. Information security: management's effect on culture and policy. Information Management and Computer Security, 2007, 14(1), 24-36.
84. Hu, Q., et al. Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture. Decision Sciences Journal, 2012, 43(4), 45.
85. Knapp, K.J., et al. Information security policy: An organizational-level process model. Computers & Security, 2009, 28(7), 493-508.
86. Herath, T. and H.R. Rao. Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations. European Journal of Information Systems, 2009, 18, 21.
87. Knapp, K.J., et al. Information Security: Management's Effect on Culture and Policy. Information Management & Computer Security, 2006, 14(1), 24-36.
88. Schein, E.H. Defining organizational culture. In J.M. Shafritz and J.S. Ott eds. *Classics of organizational theory*. New York: Harcourt Brace College Publishers, 1996.
89. Chiasson, S., et al. User Interface Design Affects Security: Patterns in Click-Based Graphical Passwords. International Journal of Information Security, 2009, 8(6), 387-398.
90. D'Arcy, J. and A. Hovav. Towards a Best Fit Between Organizational Security Countermeasures and Information Systems Misuse Behaviors. Journal of Information System Security, 2007, 3(2), 29.
91. Waly, N., R. Tassabehji, and M. Kamala. Improving Organisational Information Security Management: The Impact of Training and Awareness. In *2012 IEEE 14th International Conference on High Performance Computing and Communications*. 2012.
92. Jackson, C., et al. 2007. An evaluation of extended validation and picture-in-picture phishing attacks. In *Proceedings of the Usable Security Workshop*2007.
93. Eminagaoglu, M., E. Ucar, and S. Eren. The Positive Outcomes of Information Security Awareness Training in Companies - A Case Study. Information Security Technical Report, 2009, 14, 7.