The Curious Incidence of Security Breaches by Knowledgeable Employees and the Pivotal Role of Security Culture

Karen Renaud and Wendy Goucher

School of Computing Science, University of Glasgow,
Glasgow, United Kingdom
karen.renaud@glasgow.ac.uk, wendy@goucher.co.uk

Abstract. Computer users are often referred to, rather disparagingly as "the weakest link" in information security. This resonates with the frustration experienced by organisations who are doing their best to secure their systems, only to have an employee compromise everything with an insecure act. Organisations put a great deal of effort into education and training but it has become clear that this, on its own, is not sufficient. A wide range of relevant literature has been consulted in order to produce a model that reflects the process from ignorance to actual behaviour, and to highlight the factors that play a role in this pathway. This is the primary contribution of this paper. The model introduces the notion of two gulfs. The gulf of evaluation has the undecided user at one side, at the other a user with an intention to behave securely. A set of factors that help to bridge the gulf have been identified from the research literature. The second gulf is called the gulf of execution, which has to be bridged, assisted or deterred by a number of factors, so that users will convert intentions to actual behaviours. Interestingly, one of the factors that play a role in bridging both gulfs is security culture. Particular attention is paid to this factor and its role in encouraging secure behaviour.

1 Introduction

In days gone by "computer" security was something someone else took care of and the term mostly referred to physical access control. This was a viable approach when security entailed controlling access to the huge mainframes that did most of the computing work for the organisation. Everything changed with the advent of the Internet, connecting everyone to a vast invisible network stretching across the globe. A Google Ngrams search shows that the term "information security" first appeared in the literature in 1975, with an exponential leap manifesting from 1997 to the present time. The Internet ushered in a new era of global collaboration and easy communication but it also opened up the way for hackers to target many more machines, and to exploit the naïvety of their users and owners. This gave a hacker located in, for example, Suriname the ability to hack a Romanian computer user, without the need for physical proximity. This advance

T. Tryfonas and I. Askoxylakis (Eds.): HAS 2014, LNCS 8533, pp. 361–372, 2014.

escalated the range and number of threats as well as the difficulties of securing systems and information and made "security" far more challenging.

It soon became clear that responsibility for security was now shared by every employee in an organisation. So, instead of security being the responsibility of a select few highly trained individuals, it has now moved away from the hub and outwards to every leaf and branch of the organisation. In fact this was a positive move, because as Chia et al. [1] point out, involvement of employees in a process can, in fact, actually reduce the overall cost of security.

Organisations have responded to this reality with a two-pronged strategy. The first prong is to write and disseminate a variety of acceptable use policies which attempt to encapsulate a list of behaviours that the employees should, or should not, engage in. The second prong is the education of their employees so that they are aware of the contents of the policies, and understand how they should act to secure the information they have access to. This is reflective of the prevalent view in business: that operational training is a straightforward process of putting information in and getting the required behaviour out. In theory this sounds reasonable. In practice it hasn't worked as well as expected [2].

The new, shared, responsibility for security has not always been embraced with undiluted enthusiasm [3, 4]. Many employees see security as a hurdle [5]; something that gets in the way of their being able to satisfy their goals quickly and efficiently. It has become clear that employees, even those who have the required knowledge, sometimes still compromise the security of an organisation's systems and information by behaving insecurely. This apparent anomaly demands closer inspection.

2 Employees and Security

It is essential to understand exactly how employees are expected to assist in keeping the organisation's information secure.

If one examines acceptable use policies it becomes evident that the instructions all relate to usage. There is generally no mention of technical measures. This is an acknowledgement that many security-related activities can only be carried out by well-qualified individuals. So, for example, the IT department will install virus protection on all machines but the security policy will instruct users not to disable it. Hence it is secure usage of IT resources that is in the hands of non-IT employees. They are able to subvert security, and thereby, often unwittingly, compromise the system.

The key word in the previous sentence is unwittingly. In the first place it suggests that the employees are well intentioned and not doing this deliberately. In the second place it suggests that they simply don't know how to behave securely. Organisations thus routinely educate, run awareness campaigns, write and disseminate policies [6]. Based on the two assumptions organisations expect that employees will subsequently practice secure usage.

2.1 Security Breaches

Unfortunately, moderate to severe infractions of basic information security still happen. The Privacy Rights Clearinghouse Website[1][1] maintains a list of data breaches in the USA. It supports searching in order to examine breach antecedents. A search was carried out to extract only non-deliberate breaches that occurred in 2013. 281 (53%) breaches were returned by the search engine out of a total of 533 during 2013, the rest are attributed either to external hackers or to compromises caused by malicious insiders.

Some of the breaches were caused by errors of omission (laptops not encrypted: 36%), some are due to errors of commission (sending personal data to the wrong people: 20%) and some are due to insufficient care being taken (improper disposal of personal records 9%). Some are simply due to human fallibility: eg. loss of thumb drives (11%) and information accidentally posted on the web server (11%) and thus unwittingly made available online. Some of these seem to be a consequence of human fallibility (misdirected data) that cannot be addressed by any interventions. Others, though, could reasonably have been prevented, such as the use of unencrypted laptops outside the organisation, and improper disposal of records. It is probable that at least some of the affected organisations had policy edicts covering these aspects, that employees did not comply with.

2.2 Summary

This brief review suggests that a myopic focus on training efforts is probably not sufficient in and of itself. Organisations are keen to understand how to make their approaches more effective since breaches are damaging to their reputation and often expensive to recover from. If evidence of a better way can be provided, it is likely that they will embrace it, since they are as perplexed as researchers are by the failure of their best efforts to encourage secure usage by their employees.

It is time for us to reconsider the de facto education-based approach and formulate a new strategy. The obvious first step is to understand the employee actions, and the reasons behind them. The question that has to be answered is: "Why do employees behave insecurely despite the fact that they seem to know better?". The literature on human motivation provides insights to answer this question.

The rest of this paper is structured as follows. Human motivation is discussed in Section 3 taking a closer look at human factors that underlie behaviour. Section 4 then considers security behaviour in particular. The discussion reveals a clear distinction between behavioural intention and actual behaviour, arguing that the former doesn't necessarily lead to the latter. Sections 4.1 and 4.2 discuss these aspects in greater detail. Section 4.3 then explores the mitigating role of security culture. Section 5 concludes.

[1] `http://www.privacyrights.org/data-breach/new`

3 Human Motivation

There is a need to understand human motivation before it can be influenced. Many believe that human behaviour is easy to influence: simply incentivise the behaviour you want and punish the behaviour you don't want [8]. John Locke wrote [9]:

> *"Good and evil, reward and punishment, are the only motives to a rational creature: these are the spur and reins whereby all mankind are set on work, and guided."*

Although Locke was writing about children, this is the view ascribed to by organisations who believe that employees can be incentivised by money on the one hand, and by punishment on the other. This is a widely held belief, even in 2013, as evidenced by the many organisations who incentivise their employees by offering bonuses [10, 11]. This idea may have originated from Taylor [12] who in the early 1900s, advocated motivating workers by using external rewards. Some years later, further research revealed that when staff were paid enough to fulfill their basic financial needs [13], other aspects of the work environment also became important, such as working conditions, career prospects and flexible working hours. It turned out that Taylor was working in a time of deep depression with workers who were exerting themselves physically. His findings do not necessarily apply to knowledge-based workers in a different era.

Humans are far more complicated than is suggested by a model where extrinsic rewards motivate effort, and the greater the reward, the greater the effort. The importance of intrinsic needs must be acknowledged. Various authors have reported on a wide variety of intrinsic needs, as opposed to the extrinsic needs fulfilled by monetary rewards, which are fulfilled by employment, such as relatedness [14, 15] , moral good [16], autonomy [14, 17, 18, 15], mastery & purpose [18], personal growth & self-acceptance [19], emotional needs such as status and certainty [15] and fairness [15, 20].

There is a wealth of literature that can be consulted about what people derive from working, but since this is not the focus of this paper we will merely conclude by highlighting the oft-overlooked role of intrinsic needs, and the need to acknowledge their impact on human behaviour.

Section 2 points out that organisations' current efforts to avoid security incidents are built on two assumptions, that employees (1) are well intentioned, and (2) that insecure behaviour is due to a lack of knowledge. The rest of this paper will consider the first assumption to be true. It can be argued that fraudulent insiders have already made their minds up not to behave securely, and addressing the problems posed by these employees is outwith the focus of this paper. The second assumption has been challenged above. The rest of the paper will discuss the factors that will play a role in motivating employees to behave more securely.

4 Progressing to Secure Behaviour

Human behaviour is goal-seeking and actions are directly controlled by intentions [21]. Ajzen says "... not all intentions are carried out; some are abandoned altogether while others are revised to fit changing circumstances" (p. 2). Research suggests that, although people may formulate an intention to adhere to a behaviour in practice, they will not always do so [2]. There is thus a difference between behavioural intention and actual behaviour. An intention to behave securely is obviously a necessary prerequisite of secure behaviour, but, as becomes evident in reality, this intention sometimes does not convert to actual behaviour. Hence these two aspects should be explored separately.

In terms of information security, evidence suggests that despite the best efforts of organisations, and probably of employees themselves, these intentions do not convert to secure behaviour. If this situation is going to be ameliorated, all the antecedents, both of behavioural intention and of actual behaviour, must be understood.

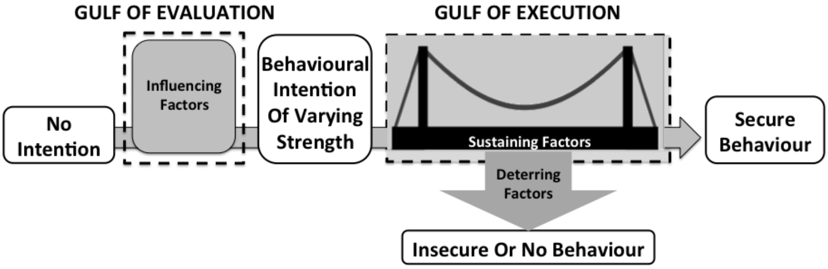

Fig. 1. Antecedents of Secure Behaviour

Figure 1 depicts the progression towards secure behaviour, with a number of factors mediating the process. The gulf nomenclature is borrowed from Norman [22] because it seems to describe the concepts expressed here so well. These two gulfs need to be traversed successfully if secure behaviour is to be realised:

- The Gulf of Evaluation: a number of factors will determine whether the person formulates the intention to behave securely or not. Section 4.1 will explore this gulf in more detail.
- The Gulf of Execution: here, too, a number of factors will determine whether the person converts the intention to actual secure behaviour. Section 4.2 will advance a number of factors that play a role here.

The factors that play a role in bridging these gulfs will probably interact with each other either to sustain or deter progress. There is no suggestion that all factors have to be active in order for the gulfs to be bridged: some may be more powerful than others, and others may only play a role in conjunction with others. Moreover, it is important to note that the behavioural intention that appears centrally is not a binary intention: it has varying strength, and this strength (valence), too, will influence whether or not the intention converts to behaviour [23]. The other aspect of intention that plays a role in how powerful it will be is its stability — how well it endures. Cooke and Sheeran [24] argue that stability might be more powerful than valence in predicting actual behaviour. As a final proviso it must be acknowledged that, in dealing with predicting human behaviour, one can never predict anything with certainty. Humans retain their uniqueness and unpredictability, which is what distinguishes them from machines.

4.1 Gulf of Evaluation

The research literature was consulted to identify the factors that could mediate in terms of encouraging formulation of the desirable behavioural intention of sufficient strength (Figure 2). To identify these factors we searched for publications that reported on the fostering of behavioural intentions in a security-related, risk-related or precautionary context. The following factors were identified:

- Knowledge [7] and Awareness [25].
- Security Culture/Norms [7,3]
- Attitude [7] which is, in turn, influenced by previous behaviour [26].
- Perceived Vulnerability [7,27,28]
- Perceived Severity [7,29,30]
- Response Efficacy (trusting in the effectiveness of the required behaviour to make a difference) [7,31,32]
- Response Cost [7,33]
- Self-Efficacy (trusting in your own abilities) [7,27]

4.2 Gulf of Execution

We carried out a search of the literature to identify the factors that would mediate in this gulf (Figure 3). We did not restrict our search to security-related publications since non-conversion of good intentions seemed to be a more wide-spread problem, and we felt that we could learn from the literature in other areas as well as the security area (diet, finance, conservation, etc.). It became clear, as we worked our way through the literature, that two kinds of factors were emerging, the first serving to increase resistance, the second acting to sustain the intention to behave securely. We therefore report these two separately.

- Deterring Factors
  - Response Cost [28]
  - Lack of Expertise (knowing what needs to be done, but not how to do it) [34]
  - Conflict between demands of job and security requirements [2]

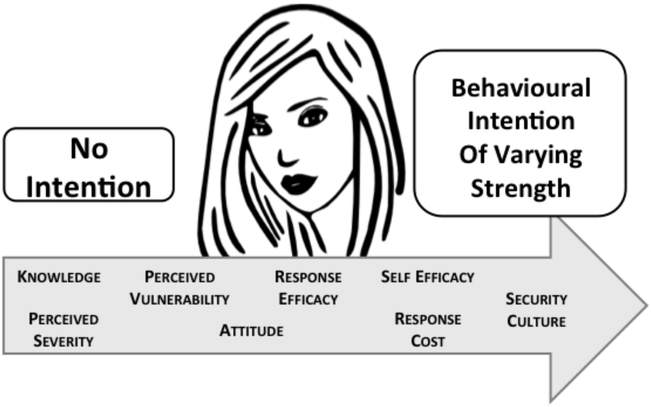

Fig. 2. Gulf of Evaluation Factors

- Scarcity of Resources supporting secure behaviour [35].
- Time lapsed since behavioural intention was formed [36, 37]
- Work Pressure [38, 34, 39, 40].
- Lack of Leadership in Organisation [41–43].
- Lack of trust in Expertise of Person advocating particular secure behaviour [44].
- Inappropriate Training eg. issuing policies without formal training [45].

- Sustaining Factors
  - Commitment to security values [38, 45].
  - Verbal Feedback on Security Performance [46]
  - Social Norms [27] and Behavioural expectations [47].
  - Employee Participation & Involvement in formulating security processes and policies [48, 1] and existence of a Feedback channel [49].
  - Visibility of Monitoring Activities [50].
  - Autonomy (having control over own actions) [47].
  - Habit (previous habitual secure behaviours make future behaviours more likely) [51].
  - Implementation intention (a plan for how the intention will be implemented) [52]

4.3 The Role of Security Culture

There is one factor that plays a role in helping the user to bridge both gulfs: security culture. It is worth taking a closer look at this particular factor since it seems to have significant potential in playing a strong role in propelling employees all the way across both gulfs to secure behaviour.

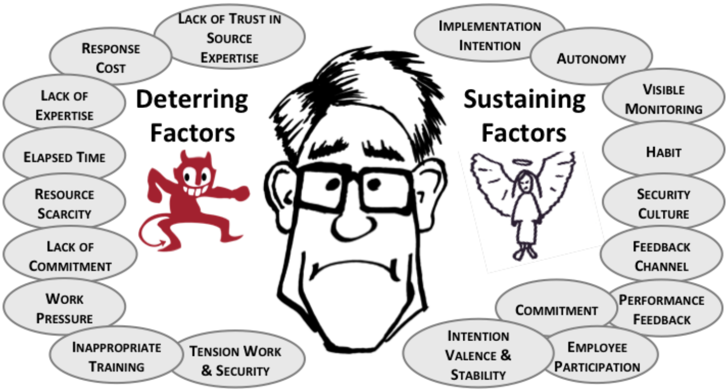

Fig. 3. Gulf of Execution Factors

A strong security culture suggests that people behave securely as a matter of course, without consciously thinking about each decision [53]. This implies that a descriptive norm exists of behaving securely, and that employees, both new and old, will be able to see evidence of this, and be influenced by it [43]. This alludes to the powerful impact of the social environment [40] and the need for active promotion of secure behavioural norms.

Van Niekerk and Von Solms [42] identify escalating levels of security culture. Knowledge constitutes the first level and this is what it makes it essential. Yet knowledge, by itself, does not constitute culture, and this is perhaps why the knowledge and training efforts of organisations have failed. Ensuring that people have the knowledge, according to the model of human motivation depicted in Figure 1 does not guarantee that a secure intention will result.

The next level, according to [42], is "shared tacit assumptions". They explain that these are shared beliefs that are taken for granted, and not necessarily verbalised. The third level is "espoused values" which are strategies, goals and philosophies which are necessarily recorded in policies that address the organisation's security needs. The final level is that of artefacts. This is in the nature of a descriptive norm [54]. Policies encode injunctive norms but these have far less impact than descriptive norms on employee behaviour.

New employees are likely to observe artefacts (cultural indicators) as soon as they start working in an organisation. These, then, constitute behavioural expectations that are very powerful in terms of guiding actual behaviour. Sheppard [55] argues that expectations might well be more influential than intentions in predicting actual behaviour.

So, how do organisations foster such norms? Feldman [56] explains that norms are constructed "through explicit statements by supervisors or co-workers, critical events in the group's history, primacy, or carry-over behaviors from past situations". Thus, verbalised behaviours coming from supervisors [43] and co-workers are important, and this is confirmed by Knapp et al. [57]. One cannot discount the impact of observed behaviour. It seems that, in addition to education and training efforts, organisations should also put some effort into discovering the descriptive norms in their organisations, especially those that have been habituated. If these are insecure, then this is an area for focused attention, in order to break the cycle before it leads to a negative security event. This can only be done effectively by observing real behaviour [57] and so short-cut approaches like employee questionnaires are unlikely to succeed.

On the other hand, the benefits of really understanding your organisation's security culture is the first step in improving it and fostering the culture you want to have. Chia et al. [1] studied security culture in organisations and make the important point that organisations should act by "emphasising that improving security is an incremental process. Instead of trying to set a short-time goal based on the level of security that you would like to achieve, set a long-term goal based on the direction that the organisation would like to follow".

The current approach of educating first and often will not, given the influencing factors uncovered in our review, change habitual behaviours that are actually descriptive norms (artifacts), which is why they propagate. It will require targeted education efforts to change such behaviours. Deliberately seeking out undesirable descriptive norms will be a valuable way of identifying areas for attention. This, then, can be followed up by deliberate interventions to bring behaviours into line with secure usage, i.e. acting deliberately to establish a security culture.

5 Conclusion

This paper has examined human motivation in general, and security behaviour in particular. Two gulfs have been identified and described: that of evaluation (formulating behavioural intent) and execution (converting intent to actual behaviour). Security culture seemed particularly efficacious since it played a role in both gulfs, so it was examined in more detail. Empirical research in this area is challenging to carry out because the stakes are so high and organisations are afraid of the consequences should an experimental new approach be harmful to security in the organisation. However, carrying out a longitudinal study of the impact of fostering clear security cultures is the obvious next step in this research now that the concept of the gulfs has been formulated and the mitigating factors identified and enumerated.

References

1. Chia, P., Maynard, S., Ruighaver, A.: Understanding organizational security culture. In: Proceedings of PACIS 2002, Japan (2002)
2. Albrechtsen, E.: A qualitative study of users' view on information security. Computers & Security 26(4), 276–289 (2007)
3. Pahnila, S., Siponen, M., Mahmood, A.: Employees' behavior towards is security policy compliance. In: 40th Annual Hawaii International Conference on System Sciences, HICSS 2007, p. 156b. IEEE (2007)

4. Siponen, M., Pahnila, S., Mahmood, A.: Employees adherence to information security policies: an empirical study. In: Venter, H., Eloff, M., Labuschagne, L., Eloff, J., von Solms, R. (eds.) New Approaches for Security, Privacy and Trust in Complex Environments. IFIP, vol. 232, pp. 133–144. Springer, Boston (2007)
5. Ross, B., Jackson, C., Miyake, N., Boneh, D., Mitchell, J.C.: Stronger password authentication using browser extensions. In: Proceedings of the 14th Usenix Security Symposium, vol. 1998 (2005)
6. Gaunt, N.: Practical approaches to creating a security culture. International Journal of Medical Informatics 60(2), 151–157 (2000)
7. Gundu, T., Flowerday, S.V.: The enemy within: A behavioural intention model and an information security awareness process. In: Information Security for South Africa (ISSA), pp. 1–8. IEEE (2012)
8. Skinner, B.F.: Beyond freedom and dignity. Bantam Vintage (1972)
9. Locke, J.: Some thoughts concerning education. In: Eliot, C.W. (ed.) The Harvard Classics, ch. XXXVII. P.F. Collier & Son, New York (1909-1914)
10. Gloucestershire Citizen, Poundland staff in Gloucester given 10p discount for Christmas bonus (December 22, 2013), http://www.gloucestercitizen.co.uk/Poundland-staff-Gloucester-given-10p-discount/story-20353454-detail/story.html
11. Hawkes, S.: IKEA rewards thousands of staff with pension bonus. The Telegraph (December 19, 2013)
12. Taylor, F.W.: The principles of scientific management, New York, vol. 202 (1911)
13. Maslow, A.H.: A theory of human motivation. Psychological Review 50(4), 370 (1943)
14. Roe, A.: Section of psychology: Personality and vocation. Transactions of the New York Academy of Sciences 9(7 Series II), 257–267 (1947)
15. Rock, D.: SCARF: a brain-based model for collaborating with and influencing others. NeuroLeadership Journal 1(1), 44–52 (2008)
16. Lopes, H.: Why do people work? Individual wants versus common goods. Journal of Economic Issues 45(1), 57–74 (2011)
17. Deci, E.L.: Intrinsic motivation, extrinsic reinforcement, and inequity. Journal of Personality and Social Psychology 22(1), 113 (1972)
18. Pink, D.H.: The surprising truth about what motivates us. Soundview Executive Book Summaries (2010)
19. Ryff, C.D., Keyes, C.L.M.: The structure of psychological well-being revisited. Journal of Personality and Social Psychology 69(4), 719 (1995)
20. Adams, J.S.: Inequity in social exchange. Advances in Experimental Social Psychology 2, 267–299 (1965)
21. Ajzen, I.: From intentions to actions: A theory of planned behavior. Springer (1985)
22. Norman, D.A.: Cognitive engineering. In: User Centered System Design, pp. 31–61 (1986)
23. Webb, T.L., Sheeran, P.: Integrating concepts from goal theories to understand the achievement of personal goals. European Journal of Social Psychology 35(1), 69–96 (2005)
24. Cooke, R., Sheeran, P.: Moderation of cognition-intention and cognition-behaviour relations: A meta-analysis of properties of variables from the theory of planned behaviour. British Journal of Social Psychology 43(2), 159–186 (2004)

25. Dinev, T., Hu, Q.: The centrality of awareness in the formation of user behavioral intention toward preventive technologies in the context of voluntary use. In: The Fourth Annual Workshop on HCI Research in MIS, International Conference of Information Systems, ICIS (2005)
26. Bentler, P.M., Speckart, G.: Models of attitude–behavior relations. Psychological Review 86(5), 452 (1979)
27. Herath, T., Rao, H.R.: Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems 18(2), 106–125 (2009)
28. Hedstrom, K., Karlsson, F., Kolkowska, E.: Social action theory for understanding information security non-compliance in hospitals: The importance of user rationale. Information Management & Computer Security 21(4), 266–287 (2013)
29. Maddux, J.E., Rogers, R.W.: Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. Journal of Experimental Social Psychology 19(5), 469–479 (1983)
30. Vroom, V.H., Yetton, P.W.: Leadership and decision-making. University of Pittsburgh Press (1973)
31. Liu, C., Marchewka, J.T., Lu, J., Yu, C.-S.: Beyond concern: a privacy–trust–behavioral intention model of electronic commerce. Information & Management 42(1), 127–142 (2004)
32. Damond, M.E., Breuer, N.L., Pharr, A.E.: The evaluation of setting and a culturally specific HIV/AIDS curriculum: HIV/AIDS knowledge and behavioral intent of african american adolescents. Journal of Black Psychology 19(2), 169–189 (1993)
33. Goo, J., Yim, M.-S., Kim, D.J.: A path way to successful management of individual intention to security compliance: A role of organizational security climate. In: 2013 46th Hawaii International Conference on System Sciences (HICSS), pp. 2959–2968. IEEE (2013)
34. Renaud, K., Goucher, W.: Health service employees and information security policies: an uneasy partnership? Information Management & Computer Security 20(4), 296–311 (2012)
35. Shelton, D.: Commitment and compliance: The role of non-binding norms in the international legal system. Oxford University Press (2003)
36. Steel, R.P., Ovalle, N.K.: A review and meta-analysis of research on the relationship between behavioral intentions and employee turnover. Journal of Applied Psychology 69(4), 673 (1984)
37. Christophel, D.M.: The relationships among teacher immediacy behaviors, student motivation, and learning. Communication Education 39(4), 323–340 (1990)
38. Whitby, M., McLaws, M.-L., Ross, M.W.: Why healthcare workers don't wash their hands: a behavioral explanation. Infection Control and Hospital Epidemiology 27(5), 484–492 (2006)
39. Bakker, A.B., Demerouti, E., Verbeke, W.: Using the job demands-resources model to predict burnout and performance. Human Resource Management 43(1), 83–104 (2004)
40. Furnell, S., Rajendran, A.: Understanding the influences on information security behaviour. Computer Fraud & Security 2012(3), 12–15 (2012)
41. Ashenden, D., Sasse, A.: CISOs and organisational culture: Their own worst enemy? Computers & Security 39, 396–405 (2013)
42. Van Niekerk, J., Von Solms, R.: Information security culture: A management perspective. Computers & Security 29(4), 476–486 (2010)

43. Leach, J.: Improving user security behaviour. Computers & Security 22(8), 685–692 (2003)
44. Pornpitakpan, C.: The persuasiveness of source credibility: A critical review of five decades' evidence. Journal of Applied Social Psychology 34(2), 243–281 (2004)
45. Furnell, S., Thomson, K.-L.: From culture to disobedience: Recognising the varying user acceptance of it security. Computer Fraud & Security 2009(2), 5–10 (2009)
46. Schelly, C., Cross, J.E., Franzen, W.S., Hall, P., Reeve, S.: Reducing energy consumption and creating a conservation culture in organizations: A case study of one public school district. Environment and Behavior 43(3), 316–343 (2011)
47. Webb, T.L., Sheeran, P.: Does changing behavioral intentions engender behavior change? a meta-analysis of the experimental evidence. Psychological Bulletin 132(2), 249 (2006)
48. Walton, R.E.: From control to commitment in the workplace. In: The Sociology of Organizations: Classic, Contemporary, and Critical Readings, pp. 114–122. Sage Publications, California (2003)
49. Singh, A.N., Picot, A., Kranz, J., Gupta, M., Ojha, A.: Information security management (ism) practices: Lessons from select cases from India and Germany. Global Journal of Flexible Systems Management 14(4), 225–239 (2013)
50. Foubert, J.D.: The longitudinal effects of a rape-prevention program on fraternity mens attitudes, behavioral intent, and behavior. Journal of American College Health 48, 158–163 (2000)
51. Ouellette, J.A., Wood, W.: Habit and intention in everyday life: the multiple processes by which past behavior predicts future behavior. Psychological Bulletin 124(1), 54 (1998)
52. Gollwitzer, P.M., Bayer, U.C., McCulloch, K.C.: The control of the unwanted. In: The New Unconscious, pp. 485–515 (2005)
53. Thomson, K.-L., von Solms, R., Louw, L.: Cultivating an organizational information security culture. Computer Fraud & Security 2006(10), 7–11 (2006)
54. Rivis, A., Sheeran, P.: Descriptive norms as an additional predictor in the theory of planned behaviour: A meta-analysis. Current Psychology 22(3), 218–233 (2003)
55. Sheppard, B.H., Hartwick, J., Warshaw, P.R.: The theory of reasoned action: A meta-analysis of past research with recommendations for modifications and future research. Journal of Consumer Research, 325–343 (1988)
56. Feldman, D.C.: The development and enforcement of group norms. Academy of Management Review 9(1), 47–53 (1984)
57. Knapp, K.J., Marshall, T.E., Rainer, R.K., Ford, F.N.: Information security: management's effect on culture and policy. Information Management & Computer Security 14(1), 24–36 (2006)