What Usable Security Really Means: Trusting and Engaging Users

Iacovos Kirlappos and M. Angela Sasse

University College London, Department of Computer Science,
London, United Kingdom

{i.kirlappos,a.sasse}@cs.ucl.ac.uk

Abstract. Non-compliance with security mechanisms and processes poses a significant risk to organizational security. Current approaches focus on designing systems that restrict user actions to make them 'secure', or providing user interfaces to make security tools 'easy to use'. We argue that an important but often-neglected aspect of compliance is trusting employees to 'do what's right' for security. Previous studies suggest that most employees are intrinsically motivated to behave securely, and that contextual elements of their relationship with the organization provide further motivation to stay secure. Drawing on research on trust, usable security, and economics of information security, we outline how the organization-employee trust relationship can be leveraged by security designers.

Keywords: trust, usable security, information security management.

1 Current State of Security Implementations in Organizations

For most people, the term 'information security' evokes technical mechanisms - such as authentication and access control - implemented to protect organizational assets [1]. Over the past two decades, awareness has been growing that many information security breaches were results of human error and social engineering; Bruce Schneier described people as the "weakest link" in the security chain [2]. Whilst some security experts have, unhelpfully, described users as stupid or careless [3], others have tried to increase compliance by providing 'more usable' security in some form. An implicit assumption of this work has been that - if people are *able* to use a security mechanism correctly, they would be *motivated* to do so [4-9]. But work by usability researchers who listen closely to users [10],[11] and economics-inspired researchers looking at cost and benefits of security mechanisms [12],[13] suggests that the assumption that 'users want security, provided it's not too difficult to use' may be wide off the mark [11],[12],[14]. Users look for efficiencies in their daily lives, and that means 'the less I have to think about security, the better'. And given that is the case, trust becomes important. The traditional "command-and-control" approach to information security management treats employees as untrustworthy components, whose behavior has to be constrained [4]. But recent research has revealed that even employees who do not comply with some security policies are motivated and act responsible when they recognize a security risk, and the cost to them is reasonable [10],[11],[15].

Thus, designers of security mechanisms should consider how trust between an organization and its employees affects security behaviors. The role of trust in technology design has been examined by research aiming to create technology platforms that enable the development of trust relationships in online commerce and gaming [16-21]. In this paper we take a different path, building on the trust model by Riegelsberger et al. [16] to explain the benefits of treating employees as trusted entities in organizational security implementations. We (1) use the model explain the creation of a trust relationship between employees and organization, (2) analyze how that affects employee compliance decisions with security policies and mechanisms, and (3) present how the organization-employee trust relationship can be leveraged by security designers to create usable and effective security implementations.

2 Trust in the Organization-Employee Security Relationships

Trust is defined as the "willingness to be vulnerable based on positive expectations about the actions of others" [22] and is only required in interactions where risk and uncertainty about the outcome exist. Risk usually arises from the potential losses a *trustor* (trusting actor) suffers if the *trustee* (trusted actor) does not behave as expected, whilst uncertainty arises from the lack of information about the ability and motivation of the trustee [16]. Both risk and uncertainty leave trustors vulnerable. The trustee's decision to behave in a trustworthy manner depends on a number of factors called *trust-warranting* properties, which can be distinguished between *intrinsic* and *contextual* [16].

- *Intrinsic properties (ability* and *motivation)*: These provide incentives for trustworthy behaviors internal to an individual. In the interaction of an employee with a security mechanism ability stems from the mechanism's usability and an individual's knowledge, while motivation comes from internalized norms and benevolence that dictate doing what they perceive to be "the right thing" in order to protect the organization they work for.
- *Contextual properties (temporal, social* and *institutional embeddedness)*: These depend on the context of the interaction and trustworthy behavior incentives for employees emerge from external factors:
  - *Temporal embeddedness* – When the prospect of repeated future interactions exist (e.g. long term future in the organization), employees are motivated to preserve the trust relationship.
  - *Social embeddedness* – When a compliant social environment exists, new employees try to fit in and mimic the behavior of others. If the majority behaves in a trustworthy manner, violations can become socially unacceptable, providing incentive to individuals to exhibit trustworthy behavior.
  - *Institutional embeddedness* – The strictness, severity and potential of punishment imposed upon an employee, together with high probability of misbehavior detection, acts as a deterrent factor to trust defection.

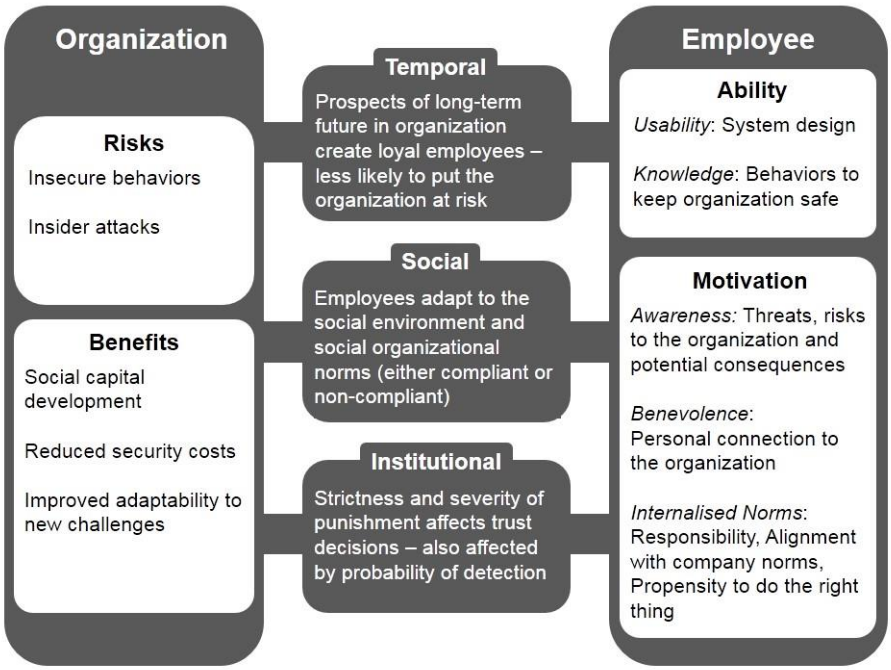

Fig. 1. The organization-employee trust relationship model
(adapted from Riegelsberger et al. [16])

3 Treating Users as Untrustworthy Components

Traditionally, information security focused on creating contextually-incentivized trustworthy behavior: imposed restrictions, controls and policies aim to create incentives for security compliance. This approach assumes users do not possess intrinsic motives to behave securely. But most employees in most organizations are trustworthy, and suggesting and they are not is counterproductive [11],[15],[23]: (i) it increases security enforcement costs, (ii) makes employees feeling untrusted, (iii) encourages creation of non-compliant environments, and (iv) negatively impacts security experts' ability to detect violations.

3.1 Enforcement is Expensive

Attempts to enforce desired behaviors upon employees increase the need for *architectural means* (security mechanisms) and *formal procedures* (policies) [24], which restrict and monitor employee actions. This increases the workload for both security experts and employees:

1. The increasing complexity of the threat landscape means defining, communicating and enforcing policy-compliant behavior to employees for all existing security challenges becomes monumental. Any attempts to achieve this become uneconomic for security experts, constrained by finite investment resources (workforce, time and budget) and may lead to security experts compromising with sub-optimal solutions [24],[25].
2. It is equally impossible for employees to memorize all approved behaviors and exhibit those in the organizational environment. Security designers, who distrust users, ask them to expend significant effort on security mechanisms. Not adopting a genuine user-centered perspective, they do not accept that security from the user's perspective is a secondary task, and that time and effort consumed eats into the users' primary task performance – and ultimately, that of the organization [12]. More often than not, users circumvent security because it gets in the way of their main job [23],[26]: users are focused on their primary work tasks and have a limited *compliance budget* for security [10] - so they try to avoid security that poses a significant obstacle to the completion of their day-to-day activities [12]. This leads to the development of insecure *informal rules* [24] and non-compliance becomes organizational security culture.

3.2 Enforcement Leads to Distrust

Treating employees as a potential threat leads to security implementations that protect from the actions of employees, who never showed any intention to damage the organization. Their non-compliance, however, stems from the difficulty to comply with security solutions that have high workload and interfere with their primary tasks [10]. For example, employees may share authentication credentials because of clear business needs: a colleague needs access to complete an urgent task, but there is no way to get credentials quickly [27]. When employees report that mechanisms are difficult or impossible to comply with, security experts tend to dismiss those reports with *'you just do to not understand the risks'* [11]. This leads to employees feeling distrusted by the security experts. Employees who are frustrated with high security overhead and do not feel trusted are likely to develop a negative attitude towards security. This leads to the creation of a *value gap* between security and production parts of an organization, and reduces employee's willingness to collaborate to keep the organization secure [28]. When that negative attitude becomes prominent, it leads to widespread non-compliance [32], insider attacks [14] and valuable employees that feel untrusted leaving organization (loss of human capital) [29].

3.3 Non-compliance Becomes The Norm

In many organizations, non-compliance has become prevalent behavior. Managers who trust their employees tolerate bending and circumvention of burdensome security policies and mechanisms. This does not mean that security is ignored: rather, employees create their own ways of keeping things they value secure, creating a *shadow security* environment [11]. This may have no resemblance to the organization's official rules, and cannot manage risks effectively, because employees do not have an accurate understanding of the risks and countermeasures. When security violations become a norm, the effects of social embeddedness on exhibiting trustworthy behavior are eliminated: new employees that try to "fit in" are more likely to follow suit to their colleague's non-compliance [30].

3.4 Ability to Detect Violations is Reduced

When rule-bending or breaking becomes an organizational norm, detection of malicious activity becomes difficult. Organization-wide rule breaking introduces significant amounts of noise in any attempts to detect suspicious activity as observed non-compliant behaviors can be both legitimate and malicious. This reduces the ability of security experts to detect and take remediating actions before the problems escalate [14]. It also makes security more expensive, requiring further investment to distinguish between 'good' and 'bad' non-compliant behaviors, further increasing the cost of architectural means to keep the organization secure [24].

3.5 Need for Trust in Security Design

The aforementioned problems suggest the need for security design to re-consider the intrinsic propensity of employees to be trustworthy: the current "command-and-control" approach does more harm than the attacks it seeks to prevent [7]. Employees possess the intrinsic properties required to behave securely: they are motivated and willing to participate in security, as long as their ability to complete their primary tasks is not significantly hindered by burdensome security

implementations [11],[14],[15],[23]. They are also capable of taking actions to protect the organization, without excessive restrictions on their systems and information access. In addition they can participate in security re-thinking as long as the experts listen to their feedback and use it to implement visible changes to the organizational security policies and mechanisms [11]. The high trust that can emerge from such an environment has social and economic benefits for the organization: it reduces the costs of compliance enforcement [24] and disgruntlement [17] (which is the starting point for most insider attacks [14] and improves organizational adaptability to the changing nature of modern security challenges [32]).

4 Incorporating Trust in Security Design

Genuine engagement of employees in security protection can have a positive effect for the organization. Collaboration builds social capital[1], creating mutual beliefs and norms which can be leveraged to improve organizational security performance [33],[34]: organizations where employees have increased responsibilities are more likely to establish a high-level of security awareness and improved understanding about the need for security. This can inject security-conscious behavior in the psychological contracts[2] that dictate employee-employer relationships, increasing the overall workforce engagement in security, and improving the effectiveness of security implementations. The emerging security consciousness also has positive economic effects on the security implementation: compliance comes from employees motivated to behave securely, based on norms developed by the existence of 'informal rules' that are significantly cheaper to enforce than formal rules and architectural means [24]. The emergent trusted environment also reduces potential disgruntlement from employees and all the potential negative effects of it (loss of human capital, insider attacks). The new dynamics that emerge can aid the organization grow especially in the new era of distributed workforce with looser and more rapidly changing organizational environments [32]. In the remainder of this section we discuss how trust can be incorporated in designing or improving security implementations, touching on four elements that currently appear to require improvements: *usability* (improving employee ability to behave in a trustworthy way), *awareness* (improving motivation to do so), *participation* (improving organizational ability to identify problems) and *punishment* (providing contextual incentives for compliance). Effective security design should aim to combine all four to balance assurance (based on architectural means and formal rules) and trust (informal rules) to create cheaper and more effective security implementations [30].

4.1 Improving Usability By Learning from Circumventions

A key requirement for employees to behave securely is the usability of security mechanisms they have to use. Security mechanisms that are difficult or impossible to use drive even trustworthy users to non-compliance [15]. Security designers and organizations need to think about usable security as a key factor of organizational *security hygiene*: rules should not have to be broken for productivity reasons. Flexibility may be available for urgent situations (e.g. give a password to a colleague who was locked out of a system), but employees should have to report these violations using an approved *controlled circumvention* system [27]. Some organizations already have *self-reporting mechanisms* that offer amnesty from sanctions to employees who self-report, but these are not helpful if self-reporting just becomes an additional task employees have to do. The causes for non-compliance have to be investigated and removed. Rules that need to be circumvented often should then be considered as unfit to support the organization. Re-designing such rules and mechanisms should be seen as essential *security hygiene*, part of an ongoing process of adapting security to fit with users' primary task and business processes [11].

---

[1] Expected collective benefits derived from cooperation between individuals or groups [31]

[2] Mutual beliefs, perceptions, and informal obligations between employers and employees [35]

4.2 Improving Awareness and Education

When security hygiene is in place, security design should build on trustworthy behavior enabled by genuinely usable security. Once that is in place, appropriate awareness campaigns to increase employee motivation to behave securely can be considered. Security designers need to identify and target current employee perceptions with context specific examples drawn from the work environment, which may differ across various employee groups [15]. The emerging communication should aim to change the perception of information security as something that protects the business process, thus presenting it as an integral part of it. This can be done by: (i) stressing the importance of security in protecting the organization and the resources that enable primary task completion and (ii) explaining the critical role employees can play in it [36]. Any education and training material used should always be easily available for employees that need to refer back to it.

4.3 Engaging With Line Managers

Line managers need to be encouraged to shape an organization's security. Security experts need to draw on their knowledge of business processes to (1) learn from circumventions and (2) get help with tailoring security awareness and make it relevant to their staff. Managers have a considerable influence on their staff's security decisions [11], and with help from security experts, they can assess the role-related risks within their teams and communicate desired behaviors. Increased awareness and ability to connect with the risks presented by their managers can provide additional motivation for employees to behave securely and can trigger internalized norms and benevolence-related compliance by employees that feel they are acting to the organization's interest. This can lead to the creation of security conscious informal rules and a security implementation based on a *bottom up* collaborative approach where employees feel trusted and motivated to collaborate in the emergent *participatory security* environment [11].

4.4 Balancing Trust and Assurance

Improvements of the trust relationship do not mean that an organization should completely abandon its deployed security mechanisms: contextual properties are also important to employees exhibiting trustworthy behavior [30]. When the ground that allows for intrinsic trustworthy behavior is created (employees are able and motivated to do so), employees should be discouraged breaking trust relationships by appropriate assurance mechanisms. Employees that are caught to abuse trust should then be visibly punished; high risk of being caught together with severe consequences has a dissuading effect for potential trust violators. In other words, organizations need to balance trust-based trustworthy behavior (based on ability and motivation) and assurance-based trustworthy behavior (based on contextual properties).

Organizations also need to recognize that, in addition to context dependent, trust is also conditional [37]: employees that have been in the organization for longer may feel more loyal, thus motivated to behave securely. Instead of all employees having to deal with the same procedures from day 1, increased levels of assurance can be implemented for new employees, with the restrictions gradually reduced the longer an employee stays in the organization – assurance should evolve to trust over time. Reducing the need for productivity-driven violations also improves the security experts' ability to protect the organization: reduction of the 'noise' introduced by productivity-driven 'legitimate' violations enables the implementation of clever monitoring implementations to identify malicious activity (insider or outsider attacks) [38].

5 Conclusion

Treating employees as a trusted entity when designing (new or improved) security processes and mechanisms can significantly benefit the organization and its security experts. It reduces the organization's exposure to information security risks by improving its security hygiene. Improved efficiency of deployed security approaches also reduces the overhead impact of security on the production tasks and employee frustration with security, creating a more positive, participatory approach to keeping the organization secure. This increases an organization's ability to depend on the human defenses (in this case employees) to manage its information security risks. Trust also improves employee attitudes, work behaviors and job satisfaction and makes security management economically more efficient, as implementation and maintenance of many cumbersome mechanisms becomes obsolete.

Improved trust relationships can emerge through: (i) improved usability of security mechanisms to improve on employee ability to comply, (ii) improved awareness to provide motivation, (iii) participatory security and middle management involvement to improve on the security designers' ability to identify and deploy improvements and (iv) monitoring and punishment to provide contextual compliance incentives – balancing all four creates an environment where trustworthy behavior is cheap for employees to exhibit and untrustworthy behavior is easily detected by the organization. This leverages employees as an additional layer of defense and improves the overall security of the organization.

References

1. Von Solms. B. “Information security–the fourth wave”. Computers & Security, 25(3), pp.165-168, (2006).
2. Schneier, B. Secrets and lies: digital security in a networked world. Wiley, (2000).
3. Sasse, M. A. Designing for Homer Simpson - D'Oh! Interfaces: The Quarterly Magazine of the BCS Interaction Group, 86, 5-7 (2011).
4. Adams A., and Sasse M. A. Users Are Not The Enemy: Why users compromise security mechanisms and how to take remedial measures. In *Communications of the ACM*, 42 (12), pp. 40-46 (1999).
5. Sasse, M. A., Brostoff, S. and Weirich D. Transforming the "weakest link": a human-computer interaction approach to usable and effective security. In BT Technology Journal, Vol 19 (3) July 2001, pp. 122-131 (2001).
6. Egelman, S., Cranor, L. F. and Hong, J. You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In Proceeding of the twenty-sixth annual SIGCHI conference on Human factors in computing systems, pages 1065-1074, ACM, New York, NY, USA, (2008).
7. Weirich, D. Persuasive password Security, PhD thesis, University College London (2005).
8. Faily, Shamal, and Ivan Fléchais. "Eliciting Policy Requirements for Critical National Infrastructure Using the IRIS Framework." *International Journal of Secure Software Engineering (IJSSE)* 2, no. 4 pages 1-18 (2011).
9. Kirlappos, I., and Sasse, M. A. Security Education against Phishing: A Modest Proposal for a Major Rethink. Security & Privacy, IEEE 10.2: 24-32 (2012).
10. Beautement, A., M. A. Sasse and Wonham, M.. “The compliance budget: managing security behavior in organizations”. In Proceedings of the 2008 New Security Paradigms Workshop pages 47-58. ACM, (2008).
11. Kirlappos, I., Parkin, S., and Sasse, M.A. Learning from “Shadow security”: Why understanding non-compliant behaviors provides the basis for effective security, in press. (2014)
12. Herley, C. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proceedings of the 2009 workshop on New security paradigms workshop* (NSPW '09). ACM, New York, NY, USA, 133-144 (2009).
13. Herley, C., "More is Not the Answer", IEEE Security & Privacy magazine, 2014
14. Cappelli, D., Moore, A., Trzeciak, R, and Shimeall, T.J.. "Common sense guide to prevention and detection of insider threats 3rd edition–version 3.1." *Published by CERT, Software Engineering Institute, Carnegie Mellon University, http://www. cert. org* (2009).
15. Kirlappos, I., Beautement, A. and Sasse, M.A.. “Comply or Die Is Dead: Long live security-aware principal agents.” FC 2013 Workshops, USEC and WAHC 2013, Okinawa, Japan, April 1, pp.70-82, (2013)
16. Riegelsberger, J., Sasse, M. A., and McCarthy, J. D.. The mechanics of trust: a framework for research and design. International Journal of Human-Computer Studies, 62(3), 381-422 (2005).
17. Hu,X.R., Lin,Z.X., Zhang,H. Myth or reality: effect of trust promoting seals in electronic markets, Proceeding of the Eleventh Annual Workshop on Information Technologies and Systems (WITS), New Orleans, Louisiana, 65–70 (2001).
18. Resnick, P.,Zeckhauser,R., Friedman,E., and Kuwabara, K. Reputation systems: facilitating trust in internet interactions, Communications of the ACM 43 (12) 45– 48 (2000).
19. Kim, D., Ferrin, D., and Rao, H. A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. In Decision Support Systems, 44(2), pages 544-564 (2008).
20. Ba, S.,Whinston, A.B, and Zhang, H. Building trust in online auction markets through an economic incentive mechanism. *Decis. Support Syst.* 35, 3 (June 2003), 273-286 (2003).
21. Nielsen,J., Molich,R., Snyder,S., and Farrell,C. E-Commerce User Experience: Trust. Fremont, CA: Nielsen Norman Group (2000).
22. Mayer, R., Davis, J., & Schoorman F. D. An integrative model of organizational trust. Academy of Management Review, 20 (3), 709-734 (1995)
23. Blythe, J, Koppel, R., and Smith, S.W. "Circumvention of Security: Good Users Do Bad Things." *Security & Privacy, IEEE* 11, no. 5: 80-83 (2013)
24. Pallas, F. Information Security inside organizations, PhD Thesis, technical University of Berlin (2009
25. Björck, F. Security Scandinavian style. PhD diss., Stockholm University, (2001).
26. Sasse, M.A. "Computer security: Anatomy of a usability disaster, and a plan for recovery." In *Proceedings of CHI 2003 Workshop on HCI and Security Systems*. (2003)
27. Bartsch, S. and Sasse, M. A. How Users Bypass Access Control and Why: The Impact of Authorization Problems on Individuals and the Organization, ECIS2013: the 21st European Conference in Information Systems (2013).
28. Albrechtsen, E., and Hovden, J. The information security digital divide between information security managers and users. Computers & Security 28, no. 6: 476-490 (2009).
29. Morrison, E. W., and Robinson, S. L. "When employees feel betrayed: A model of how psychological contract violation develops." *Academy of management Review* 22, no. 1: 226-256 (1997)

30. Flechais, I., Riegelsberger, J., and Sasse, M. A. Divide and conquer: the role of trust and assurance in the design of secure socio-technical systems. In *Proceedings of the 2005 workshop on New security paradigms* (NSPW '05). ACM, New York, NY, USA, 33-41 (2005).
31. Hanifan, L.J. "The rural school community center." *Annals of the American Academy of political and Social Science* 67: 130-138, (1916).
32. Tyler, Tom R. "Trust within organizations." *Personnel review* 32, no. 5:556-568. (2003)
33. Bussing, A. "Trust and its relations to commitment and involvement in work and organizations." *SA Journal of Industrial Psychology* 28, no. 4 (2002).
34. Tsai, W., and Ghoshal, S. "Social capital and value creation: The role of intrafirm networks." *Academy of management Journal* 41, no. 4: 464-476 (1998).
35. Rousseau, D. M. "Psychological and implied contracts in organizations. "*Employee responsibilities and rights journal* 2, no. 2: 121-139 (1989).
36. Von Solms, B., and von Solms, R. From information security to business security. Computers & Security, 24(4), 271-273 (2005).
37. Castelfranchi, Christiano, and Rino Falcone. *Trust theory: A socio-cognitive and computational model*. Vol. 18. John Wiley & Sons, (2010).
38. Caputo, D., Maloof, M., and Stephens, G. Detecting insider theft of trade secrets. Security & Privacy, IEEE, 7(6), 14-21 (2009)