Human Factors and Information Security

Lewis Hassell  
Drexel University  
College of Information Science and Technology  
lew.hassell@cis.drexel.edu

Susan Wiedenbeck  
Drexel University  
College of Information Science and Technology  
susan.wiedenbeck@drexel.edu

Abstract

Security, including information systems security, is a societal problem, not just a technology problem. Getting people to adopt secure IS practices requires more than traditional ease of use studies and user requirements analysis. It requires users of advanced information systems to adopt a culture of security. We propose a model of organizational security, which includes user security behavior as a key element. Next, we propose a model of user security behavior itself, and discuss how it shows how we have to create this culture of security. Lastly, we discuss directions for future research.

1. Introduction

“[Using home security as an analogy] 95% of security problems are caused by casual walk-in burglars who find you don’t bother to shut all the windows and doors when you go out, while only 5% come from more devious and determined thieves ... It’s only when a culture of security is instilled into an organization – so that every employee is aware of security measures and why they have been put in place – that security can be effective.” Paul Rubens, Building a Blueprint for Network Security

The above quote could just as readily have come from a thousand other books, journal articles, or web sites. Everyone knows that changing the way people – ordinary people, not computer scientists or engineers – think about security is the key to the central information security problem: even if end users are aware of security issues, they may not act on them. This means that no matter how good the technology of security is, its use will continue to be suboptimal. Even in federal government agencies, where one might expect to find information security taken seriously, the situation has gotten so bad that the Office of Management and Budget has told 18 agencies not to develop, modernize or enhance IT systems until their cybersecurity problems are fixed [23]. Despite the fact that non-technical computer users are the weak link in information systems security, the study of human factors on security compliance has remained largely ignored in Information Security (INFOSec) and Information Assurance literature. It seems that there is an implicit assumption that enough technology will solve the problem – that if we can only remove humans from the equation, we can automate our way to information systems security. While technology is certainly important, the assumption that it will solve the security problem has yet to be justified, and is, in fact, denied by the HCI expert, Jacob Nielsen [22]. Furthermore, it ignores the common dictum that security has three parts: technology, process and people.

In this paper we will be drawing no distinction between Information Assurance and Information System Security. While the NSA and other organizations consider the difference significant (and rightly so), for our purposes it is unimportant. This paper will argue for the assumption that changing the way people conceptualize information systems security will change the way people act. In turn, this will create a culture of security. We will then propose a model concerning the creation of this culture. But this is not a model of how to manage the way end users think about and act on computer and information security. It will be a model of shared responsibility – indeed, ownership – of information security.

Specifically, this model will take into consideration the human issues surrounding information systems security. What are the perceptions of information systems security by the non-technical user? How do they respond to security alerts? What factors affect their compliance with security issues? How important do they perceive security to be? Why should the ordinary computer user care about security? This model will impact how to address, change, and manage those
perceptions to align with what the INFOSec community knows is needed. In addition, it will address what organizations require of security-related behavior in the context of humans as social creatures, not specifically as users of technology. The underlying assumption is that ease of use is not as important as social acceptance. We will thus look at ‘compliance’ not from the point of view of obedience but from the point of view of human beings doing that which defines them as human – participating in a community, a culture. Indeed, it has been noted (e.g., [12]) that information security tends to become an industry practice (i.e., a set of policies and procedures), not a customer-centric culture.

2. Information Security Related Definitions

Information Assurance (IA) may be defined as information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. [DOD Directive S-3600.1, 1996]. INFOSec is defined as the protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional [FS 1037C, 1996]. IA, then, is broader than INFOSec. IA is thus preferred to INFOSec according to the National Security Agency. For our purposes we will treat “information assurance”, “information systems security”, and “information security” as equivalent terms.

3. Review of the Literature

We will review literature from three separate fields, each of which adds its own distinct and important element to the theory underlying the model. These three fields are the body of literature concerning HCI and information systems security, diffusion of innovation theory, and communication theory.

3.1 System Usability and Security

To date there has been some small discussion of the importance of end-user attitudes toward security [28]. Most of the discussion has had to do with how to get non-technical users to follow good password regimens.

Sasse [3,5,31] has looked at user interface issues related to passwords. She [31] found that fear was a useful mechanism for getting people to follow password policies. They did not, however, examine whether fear is an entirely appropriate mechanism, or even if it achieves its desired goal of positively impacting organizational security. Nor did they consider whether fear is the technique of choice for the long term? Lastly, employers may be able to use fear of dire consequences for one’s job if one does not follow certain security practices at work. Extending this to home computer use remains problematic. This is certainly a problem given the fact, for instance, that most distributed denial of service (DDoS) attacks are based on zombie networks, some of which consist of up to 140,000 home computers [13].

[31] also explored techniques derived from social marketing. Social marketing is based on the idea that the same marketing principles that were being used to sell products to consumers could be used to sell ideas, attitudes and behaviors. These techniques were useful for associating positive personal qualities (such as caring) with good password practice and associating negative personal qualities (such as self-centeredness or laziness) with bad password practice. The question as to whether any attention paid to users will result in increased compliance – or productivity, as in the case of the Westinghouse effect – was never addressed. (The Westinghouse effect refers to an experiment in which a researcher went into a Westinghouse plant to try to find psychological ways of improving production. The researcher found that whenever he set up studies and made observations, production increased. The final conclusion of the Westinghouse study was that attention given to workers at the plant seemed to increase productivity because people like attention.) Furthermore, we must wonder how long the behaviors will last or will the change in behavior be ephemeral.

Zurko and Simon [32] and Besnard and Arief [8], among others, talk about user-centered security. Like many who discuss the user-centeredness of technology, they are looking at humans not propter se but as users of technology. Their work focuses on usability as the primary goal of the design of systems – the number of errors committed, the time to completion of a task. They did not examine the social organization and communication patterns that underlie the diffusion of new technology and they ignore the social context in which these systems occur.

Anne Adams [1,2,3,4] addressed social issues in security, but only concerning privacy. That is to say, she discussed the risks to personal privacy that security infractions can result in. Adams also addressed the issue of password security ease of use [5], but not the social or organizational context.

Schultz [29] proposed a taxonomy of usability for security controls and why each element of the taxonomy was necessary. Their analysis, however, centered on technology and task, not on the sociotechnical system that is the foundation of all organizations and organizational activity. They note that “(m)ost (if not all) security-related controls rely on individuals to
implement and deploy them” (621). They miss the fact that security exists for the sake of humans and their systems.

What almost all of these researchers have in common is that they are largely concerned with improving password creation and use. Information systems security is far broader than passwords. We certainly need advanced techniques for password creation and use, cryptographic systems, email filtering, personal firewalls, software patch maintenance. Equally important, or perhaps more important, we need to understand how to integrate them into a culture of security.

3.2 Diffusion Theory

Diffusion of Innovation Theory [25] – Diffusion Theory, for short – concerns itself with the way in which new ideas/technologies disseminate through a culture or group. According to Diffusion Theory, technological innovation is communicated through particular channels, over time, among the members of a social system. This occurs in five stages: the knowledge of the existence of the innovation, the forming of a favorable attitude, the decision to adopt, implementation, and its reinforcement based on positive outcomes. Furthermore, the five adopter categories are innovators (adventurous), early adopters (respectable), early majority (deliberate), late majority (skeptical), and laggards (traditional).

Key players in getting a community to adopt an innovation are opinion leaders (who have relatively frequent informal influence over the behavior of others), change agents (who have a positive effect on innovation, by mediating between the change agency and the relevant social system), and change aides (who complement the change agent).

Rogers’ communication model for the diffusion of innovation is the (S-M-C-R-E) communication model. In this model, the Source (or Sender) conveys a Message via a Channel to a Receiver with the explicit purpose of establishing a change in the knowledge, attitudes and, ultimately, the behavior or practices of that Receiver (Effect).

Diffusion Theory has been applied to and used to extend a myriad of disciplines and areas within information technology (e.g., [7], [9], [15]). As yet it has not been applied to the field of computer and network security (or, more broadly, information assurance). We believe that simply thinking about security in these terms would bring a great advantage. Moreover, research into the diffusion of security knowledge and compliance would itself inform and extend Diffusion Theory.

3.3 Communication theory and sociolinguistic research

The concept of “common ground” is a well established one in the field of communication [10,11] and one that has had enormous impact on many fields, including the IT-related fields of HCI and CSCW. In any collaborative activity, especially those involving the dissemination and adoption of new ideas, it is important to come to an adequate level of mutual understanding. To achieve this, individuals must share mutual understanding, knowledge, beliefs, assumptions and presuppositions. The interactive process during which this mutual understanding is created is called “grounding”. Some degree of “common ground” may already exist between two individuals – that of a shared culture, for instance. Each “layer” of knowledge or activity, then, requires additional grounding.

The concept of common ground does not conflict with the S-M-C-R-E model of Innovation Theory but rather complements it. Common ground elucidates the importance of the relationship between the Source and the Receiver and the consequent Effects. It is difficult or impossible for an outsider to introduce innovation into a society. Opinion leaders, change agents, and change aides cannot mediate between the change agency and the social system if they are seen as outside the social order. Those who are seen as not having much in common with us are seen as “outsiders” and tend to be distrusted. People who know one another can use their common ground to create more successful conversations, whereas strangers need to make their statements and presuppositions more explicit [14]. An important question is whether the IT community can ever become change agents, or if they must look to recruit change agents from within the user community. Does the end-user community hopelessly see information system professionals as “geeks”? Or worse, does the end-user community see information system professionals as being disdainful of them because of their relative lack of knowledge of computer and telecommunication technology? The concept of grounding thus should provide fertile “ground” for the discussion of how to obtain culture-based compliance with security procedures.

The use of language involving change management and persuasion has been studied, but largely in fields outside IT. In an exception, Hassell [17] has demonstrated that indirection, a form of politeness, features large in interpersonal communication, within software teams. That is, requests and commitments were usually made in a way that would permit both parties, requestor and promisor, to “save face” should some problem in the transaction arise. Furthermore, the same research also showed that email patterns of communicative interaction differed considerably from
those of face-to-face. Thus, the use of language can affect the social interaction between coworkers. How this might impact compliance with security measures is yet to be determined.

4. Toward a model of Human Factors and Information Security

Creating models is an important part of IT. It permits us to abstract from reality and determine what is important to the domain in which we are working. As yet, no model of organizational security has arisen, nor has a model arisen of information systems security. Thus, we now propose a preliminary model of organizational security (of which information systems security is a part). Next, we propose a model of user security behavior.

4.1 Model of organizational security

Understanding information systems security from the rational choice model [6] has been suggested. Under this model, people are to a greater or lesser extent guided by a rational tradeoff between the probability of the success of a behavior and the desirability of the choices involved. While there might be something to be gained from this, we believe such approaches fall far short of what is needed because humans are not completely – or even largely, governed by reason. Instead, social systems are open, dynamic, and made up of many non-rational elements [26]. Any model of human interaction, including – indeed, especially – regarding security matters must take this into account.

Figure 1. Model of organizational security

Figure 1 shows our proposed Model of Organizational Security. A number of elements must be highlighted. Management Support is the *sine qua non* for any successful business endeavor. Therefore it influences both IT and user security behaviors. On the other hand, External Business Factors, such as business competition and product development are difficult to predict, but we must remain sensitive to their possibility and influence on Organizational Security. IT Factors and User Security Behavior are important and influence one another, as we will discuss in more depth below. We may assume that External Business Factors affect User Behavior insofar as they affect the business environment to which the user responds. Technology obviously influences IT. In an ideal world, there would be no technological innovations that were not addressed by IT. Physical Security affects information systems security but seems to be more addressed in professional conferences and magazines than in the academic sphere. External Global Factors, like cyber terrorism, all have an impact on Organizational Information Systems Security.

4.2 User security behavior

Figure 2. Model of user security behavior

Figure 2 depicts the characteristics that we need to study in both the end-user arena and in the IT arena. There are, of course, technical factors that pertain to IT. What is often overlooked, however, is that they are actors, just as end users are. If their values, knowledge
and commitment to the organization are not taken into consideration when rolling out any technological innovation, problems will surely result. Personal values are important to both the end user and the IT personnel. Both must have a collaborative work ethic, be team players, and see a good greater than themselves.

Both IT personnel and end users must also exhibit common sense. But what an individual views as common sense has to do with personal values and socialization. Thus, the farther apart that IT and users find themselves, the farther apart they may find their respective views on common sense.

4.2.1 IT factors

Let us assume that most of what is written about technology falls outside what we are referring to as IT Factors. It is properly the domain of Technology in our Model of Organizational Security. Other than technical competence of the IT staff, then, the topic that is most often written about in this regard is training. Making users aware of security mechanisms, according to this reasoning, is what we need to do to get users to comply with security procedures. The correlation between education and increased security has yet to be established experimentally. In calling for expanded research into security training, for example, Schultz [28] notes skills and training. But one cannot acculturate an employee to the organization’s security culture with a ½ hour HR lecture/film and a manual, or with periodic classes on what they are doing wrong. What we need is less training (though that would be of some help) than teaching employees to participate in a culture of security. The essence of this sort of education is that all parties involved have some common ground – i.e., they share values, assumptions, and underlying knowledge.

We must be clear that this form of education and culture transcend the IT department, something that is often lost on IT personnel. Consider Doughty [12], “An organization’s culture is often imprinted not only into the management practices i.e. policy, procedures and directives, but also on its personnel, particularly if the personnel involved in system development, project and operational management have been long-term employees of the business” (p100-101). This is precisely not the case. The IT unit of an organization is often not in touch with the culture of the organization as a whole, and as a result its members are viewed as outsiders.

4.2.2 IT human factors

What is generally not discussed much concerning security is the general reputation of the IT department within the organization. When we speak of reputation, we go beyond competence and dedication to one’s job. IT probably does not deserve the bad rap it gets [24]. On the other hand, it seems true that IT does have a bad reputation within organizations. Many anecdotes attest to the general lack of regard in which IT groups within organizations are generally held. A graduate student of mine (a professional developer) told me that end users sometimes “lack the vision” to see the “virtues” of her applications. The fact that we tend to side step the issues surrounding the reputation of IT in organizations is demonstrated in studies where the success or failure of strategic information systems is determined by IS personnel, not the users [16]. Even in studies that included non-IS personnel in their survey (e.g., [27]), they were outweighed by IS personnel and no factors concerning the general reputation of the IS department were considered.

Thus, the question becomes, if the IS department is, in fact, not in high regard, what are the chances that they will be listened to when they issue information security statements?

4.2.3 End user human factors

Since end users are humans just as IT personnel are, there is not much difference between the human factors of the two. The one obvious difference is that with end users it is the strength of organizational culture and values that is significant. With IT personnel, the question is how and to what extent corporate culture and values are integrated. The reason we make this distinctions is this. If organizational culture and/or values are weak, then there will always be difficulty in getting users to follow any organizational mandate. They will not be inclined to be team players. On the other hand, if the members of IT do not identify themselves first and foremost with the organization, then they will not be readily trusted and their ability to effect change will be diminished.

It must be recognized that Business Security affects and is affected by Home System Security. For instance, an organizational server connected to a home machine via a VPN is only as secure as that home computer is. If the user at home is negligent of good security practices, the home system, and consequently the organization’s server, may be compromised. This simple, but powerful, fact is often ignored in discussions of business security, though not on the Computer Emergency Readiness Team (CERT). We have not directly represented it in our model because viewing the end user as a complete human being will, in the end, reflect in computer behavior at work and at home.

4.2.4 Evolving the model

Interestingly, the highest impact areas of potential research represented by the models are not the nodes but
the edges connecting the nodes. These nodes represent the “how” of the interaction of factors. And it is here that the equation becomes more complex, because the weights assigned to the various factors, and their ultimate influence on the equation, get taken into account. It appears that the factors are not merely additive, but interact in multiplicative ways.

It is in the edges, for instance, that we find the impact of language. Much research in IT takes a somewhat naïve view of the use of language. Hassell [17], for example, has shown that “face management” [18] is important in project interaction. Face Management refers to the process that goes on in conflict where both parties are concerned with maintaining their social status during an interaction. The ways in which you can achieve this goal include appearing smart, honorable, right, or warranted in your stance. Also, the same research shows that there are considerable linguistic variations in the same interactions given different media.

We see the interface between the values held by IT personnel and the organizational values held by the user population as the area of possible common ground for both parties. This intersection of values will also impact on what they each view as common sense. Building this common ground is closely related to the concept of the diffusion of innovation, for it is only insiders that can be opinion leaders, change agents and change aides. And where IT has traditionally struggled, and security has remained curiously silent, is in the creation of these sorts of partners for change among the end-user population.

Research in other domains (e.g., [19]) has outlined the possible roles of a change agent. Depending on the organization and context, change agents may act as one or more of the following: enablers, catalysts, solution givers, process helpers, stimulator-innovators, resource linkers, brokers, gatekeepers, social-interactionists, and advocates. Detailing the specifics of each role is outsider the scope of this paper. Suffice it to say that these roles must be taken by end users, but must be nurtured by IT. IT must recruit respected members of the end-user community who are well known, facile at social interaction, and likeable. They must then provide them with the knowledge and tools to make them successful information security advocates. One should not think, however, that this eliminates the need for close alignment of IT personnel’s values with those of the rest of the organization. Nothing could be further from the truth. Close alignment is crucial in order to recruit end-user change agents to begin with.

The authors that perhaps come closest to our ideas are Vroom and von Solms [30] and Leach [20]. Vroom and von Solms suggest that emphasizing alignment with corporate culture might be a replacement for, or at least supplement to, security auditing. Their analysis stands in need of supplementation for several reasons.

They assume, like Leach, that values are cognitive. They assume that all values, organizational norms and knowledge are necessarily, or even mostly, conscious. Researchers like Lewicki [21] have largely disproved this. Lastly, they assume (implicitly) that the fundamental level of analysis is the individual.

Leach [20] talks about the body of knowledge (which include organizational values) and the user’s personal values that influence user security behavior. He ignores the fact that values are in the arena of affect and socialization. Leach also appeals to common sense, but as we said in our discussion of common sense (section 4.2) above, what a person views as common sense is very dependent on their own base knowledge, their own world view and their own value system.

5. Conclusion and Recommendations

If our models are correct, then it implies that technology solutions alone to security are completely inadequate. Social, organizational, and psychological factors must be considered when implementing security within an organization. We will have to consider how people build communities. We will have to take into consideration how communication patterns affect interactions.

Future research should include:

- What is the reputation of IT in organizations? At what levels within the organization? How does it differ from IT’s self perception? How can it be enhanced?
- What is the payoff of increasing the reputation of IT overall versus applying diffusion theory concepts to security?
- What is the importance of centralized IT versus decentralized IT for security? This would parallel the discussions of centralized versus decentralized IT.
- What weights should be applied to the edges that connect the factors affecting security in the Model of Organizational Security?
- What types of change agents are most effective in “spreading the word” of information security? How does IT cultivate them?
- Short of teaching psycholinguistics to IT personnel, how can we make use of research in communication to influence users and enhance IT reputation?
- What sort of communication media should be used in communicating with end users?
- How do the characteristics of communication specific media impact IT communication, particularly with respect to security?
A final issue not directly addressed above is how to interact with management and how do we engender a culture of security among them. Spreading the culture of security to them may be the same, or it may be different, as to other parts of the organization.

In the end, we believe that threats are of no use. Even if threats do work in a business environment, they can only breed resentment, and there is absolutely no reason to believe that the desired behavior will be translated over to one’s personal behavior with one’s home devices. And it seems almost a truism that if home PCs, cell phones, and PDAs are not secure, then the Internet and the rest of the world’s information infrastructure are not secure.

Furthermore, if the technical staff does not engender a culture of community in non-technical end users, it cannot create trust and a desire to cooperate that is needed to create a culture of security.

6. References


