# Organizational Transformation and Information Security Culture: A Telecom Case Study

Gurpreet Dhillon, Romilla Chowdhuri, Cristiane Pedron



# Organizational Transformation and Information Security Culture: a telecom case study

Gurpreet Dhillon[1], Romilla Chowdhuri[1], Cristiane Pedron [2]

[1]Virginia Commonwealth University, Richmond, USA
{gdhillon, syedr2}@vcu.edu
[2]University of Lisbon, Portugal
cdpedron@gmail.com

**Abstract.** When two companies merge, technical infrastructures change, formal security policies get rewritten, and normative structures clash. The resultant changes typically disrupt the prevalent security culture as well. In this paper we use ET Hall's (1959) theory of cultural message streams to evaluate the disruptions in security culture following a merger. Findings from our analysis would be beneficial to researchers to theorize about security culture formulation during a merger. At a practical level decision makers would find the analysis useful for engaging in strategic security planning.

**Keywords.** Security Culture; Organizational Transformation; Formal & Informal security

## 1 Introduction

The merger of the companies cause significant challenges in terms of integrating their technical infrastructure, policies and procedures, and normative aspects related to how work gets done. The changes also have a consequent effect on the security and integrity of the enterprise. Previous research shows (see [2], [8]), that structural and business process related changes indeed make an organizational vulnerable. Research also shows that building and sustaining a good security culture is extremely important in times of radical change. In this paper we use E.T. Hall's theory of cultural messages [4] to evaluate information security consequences of an organizational transformation

In the extant literature, security culture is deemed important for the protection of organization's information assets. Various definitions of security culture have been proposed. For example, Dhillon [2] defines it as behavior, values, and assumptions that ensure information security. Helokunnas and Kuusisto [5] define security culture as a system in which attitude, motivation, knowledge, and mental model about information security interact. With respect to organization's information as-

sets, researchers express the need for coherent security culture that focuses beyond the technical and formal controls [2], [7], [9], [10]. Recent literature review by Ramachandran et al. [6] indicates that very few studies focus on security culture. Moreover cultural conflict in information security has not been studied very well.

## 2 Case Description and Analysis

In this study we adopt an interpretive case study research approach [11]. Data was collected primarily through semi-structured interviews and informal conversations. Participants were the employees at different management level in the two merging companies. The participation was voluntary and each interview lasted about 60 minutes. Majority of the data was collected over an eight-month period while the merger was in progress.

The setting of the case study is an Organizational Customer and Relationship Management (OCRM) project that was launched due to the merger of the two companies - AirTelco and Relicom. The project aims to support the business goals of the transformed organization by integrating the CRM systems of the two merged organizations. Both AirTelco and Relicom belong to a business group that is greatly projected in Europe and has diversified business portfolio. Relicom was the industry leader of landline phones. The company offered its customers a wide range of services and solutions that cover more than the normal fixed network services like data communications, broadcasting, video conferencing, and broadband solutions. AirTelco was the market leader of the mobile segment. Its main goal is technological innovation and customer orientation. The differences in the strategic focus of the two companies stem from how they originated. While AirTelco was a product of a competitive market space, Relicom grew up in a monopolistic market. These differences in origin were evident in the approaches that the two companies had adopted towards technological innovation and customer management.

The cultural map analysis is performed using E.T. Hall's ten streams of cultural messages. The interpretations about the impact on information security are drawn by reflexive thinking in relation to cultural messages and data provided by the participants. Per our analysis, *gender* did not

emerge to be significant. The summary of the analysis is presented in Table 1.

**Interaction**. The OCRM project affected the interactions between the higher management and operational teams. Inclined towards technological innovations, AirTelco employees occupied dominant technology positions whereas Relicom employees occupied managerial roles. This segregation of technological and managerial roles not only created division of power and space but also caused a lack of clarity in terms of privacy and security of customer data that resided on OCRM servers.

**Association**. As the two organizations had different approaches towards customer management, a sense of sub-communities caused resistance towards adopting OCRM. In addition, lack of governance structures further increased the distance in security culture.

**Subsistence**. Although employees were trained for using OCRM, no knowledge about the changes OCRM instigated in the business processes was disseminated. OCRM was of little to employees in overcoming their comfort zones. Additionally, the legal and regulatory differences prevented the integration of some of the databases, leading to information availability and integrity issues.

**Territoriality**. The OCRM system defined new work boundaries for AirTelco and Relicom employees. Relicom employees felt that they were forced to follow the division and space determined by AirTelco employees. Work remained compartmentalized, formal boundaries changed and new group boundaries emerged. Such hostility between groups makes them prone to social engineering attacks.

**Temporality**. The requirements for the design and implementation of OCRM system were collected in just five weeks. Additionally, AirTelco employees had a laid back attitude in dealing with day to day issues whereas Relicom employees were more aggressive. There were frequent changes in the process and people involved in requirement gathering. As a result, employees were inventing unique ways of getting work done faster.

**Learning**. Few employees were selected to give training to other employees. However, the manuals put together by trainers were based on what they wanted others to know. Training between AirTelco and Relicom was not synced. Relicom for example knew more about wireless products and services relative to AirTelco. Training was limited to technical knowledge; employees were not made aware of the security policies.

**Table 1.** – Cultural Analysis Mapping

| **Direct Organizational Intervention through the OCRM system** | **Implications for Security** |
|---|---|
| Interaction: Communication patterns changed because people from both companies need to work together formally and informally.OCRM forces AirTelco and Relicom to cross sell and be customer responsive. | Lack of clarity in terms of security and privacy. New organization had limited grip on protection of critical company and customer data. |
| Association: Prior to merger, AirTelco and Relicom had multiple groupings and perspectives for CRM implementation. Conflicts were rampant. Merger of two companies results in "them" vs. us" attitude. | Conflict among groups was rampant. This resulted in lack of agreement on the kind of controls that were to be established.<br><br>Absence of formal associations caused a lack of shared vision which is detrimental to system success. There was no sense of ownership about customer data. |
| Subsistence: Prior to the merger, AirTelco employees had very little interest in customer service because a) it was difficult to cross sell products/services b) performance was loosely linked to employee earnings.<br>Following the merger, however lack of customer responsiveness and inability to sell telecom services would result in reprimands. At the same time OCRM made sales and service efforts easier. | While the merger took place, the databases of the two companies cannot be merged because of legal and regulatory reasons. This results in issues pertaining to management of security, data integrity, and availability. |
| Territoriality: Following the merger, Relicom employees felt that they had to follow the divisions and space allocations of AirTelco. Merger brought two companies to share resources and equipment. The manner in which they approached work remained compartmentalized. | A lack of clarity of business processes, formal and informal spaces creates issues regarding 'social obligations' and 'responsibilities' that go beyond the law of the letter. Typically such environments can be excellent candidates for social engineering attacks/manipulations. |
| Temporality: Requirements for the new OCRM were collected in just 5 weeks and every few weeks the process and responsibilities changed. AirTelco had a more laid back attitude in dealing with issues, problems and customer complaints, while Relicom was more aggressive. | One of the biggest concerns with respect to temporality is flawed assumptions leading to incorrect specification. The flawed or buggy systems are not only costly and time consuming to fix, but also pose significant security hazards.<br><br>Frequent changes in routines results in human error, which is a serious security threat. |
| Learning: Learning was undertaken in 'train the trainer' mode. The training program was technical in nature. Employees were however left to themselves to articulate the training content. In many instances new products and services were offered without adequate training or making employees aware about such products or services. | The nature and scope of training impacts the kind of a policy that is developed. If the new company wanted to create well balanced security policies, their training should go beyond the technical edifice. However, this was not the case. While employees seemed to be well versed with the technical, products, and services, they were unsure if the processes were broken or routines were inappropriate. This is a serious security threat because of exclusive reliance on the technical fix. |
| Recreation and Humor: Post merger the company created a "stock market" for ideas where employees could invest their virtual money. | Creating homogeneous culture for ensuring security is always preferred. The new AirTelco/Relicom organization did a good job in creating such an environment. However, there was no means for them to ensure con- |

| | |
|---|---|
| | tinuous improvement and integrating cultural process back for a sustained cultural integration. Failure to do so usually causes disillusionment and results in employees abandoning their integrative efforts - a serious security concern. |
| Defense: OCRM enforces formal controls on employees. Employees were expected to comply with the inbuilt controls. | The manner in which the changes panned out or were interpreted resulted in discordance between different stakeholders. Employees seemed to be at the mercy of the newly established routines. While this was necessary at the lower end of the organization, managers themselves felt that OCRM imposed an over-engineered solution. Increased possibility of employees circumventing control, which is a major security issue. |
| Exploitation: The organization (post-merger) has created a "laboratory of new ideas". Employees from different divisions are encouraged to brainstorm and test the efficacy of new ideas. | While the intent of the laboratory was very good, it received mixed reviews. In some cases employees felt involved, but in others they seemed to be disillusioned. Organizations need to ensure sustainability and correct direction of such innovative arrangements in order to ensure correct exploitation, else there is a risk of failure/abuse. |

**Recreation and Humor.** To facilitate cultural homogeneity between employees, senior management encouraged employees to discuss investment options. However, there was no effort made to improve such interaction. Failure to do so usually causes disillusionment and results in employees abandoning their integrative efforts.

**Defense**. Although, inbuilt controls in OCRM ensured security, these formal controls imposed restrictions on employees and forced them to work as per defined processes. Employees learned to circumvent the system to ensure that the work gets done as per their way.

**Exploitation**. A “laboratory” setting was created to allow employees discuss innovative ideas. In some cases employees felt involved, but in others they seemed to be disillusioned. Although innovative ideas were generated and implemented, few of them were pushed through because of the power of the people who promoted those ideas.

## 3 Discussion

The case study presents an interesting basis for interpreting silent messages and hence the prevalent security culture. Based on our analysis we identify several principles that form the basis for good information security management.

1. *Good information security management is a function of effective communication structures.*

While the need for establishing communication structures may seem intuitive, the importance of such structures in ensuring good information security cannot be underestimated. It was Giddens [3] who proposed that two disembedding mechanisms exist - tokens and expert systems. For Giddens tokens is any media of interchange that could be passed from one place to the other such as physical artifacts, conceptual structures or information. In the context of the merger between AirTelco and Relicom, while the OCRM system could have been a token, there clearly was significant confusion regarding how the system could be used to ensure customer responsiveness. On the contrary, the system imposed its own way of working and hence created confusion amongst the stakeholders. In the literature, the importance of tokens has been noted as significant as they ensure a common basis for establishing a communication structure (see [2], [3]).

The second disembedding mechanism noted by Giddens [3] is that of expert systems- a collection of people who have specialized knowledge. While the merger between AirTelco and Relicom went ahead and various systems were inherited, there was no effort whatsoever in establishing expert systems. Hence conflict among groups was rampant, which resulted in lack of agreement on the kind of controls that should be established.

2. *Information security management is a consequence of how business processes are redesigned taking into consideration the informal, formal, and technical aspects.*

Hall [4] argues, “Change is a complex circular process. It proceeds from formal to informal to technical to new formal, with the emphasis shifting rather rapidly at certain junctures” (pg 93). It is interesting to note that both AirTelco and Relicom recognized the importance of creating a homogeneous culture, which would ensure security. The new AirTelco/Relicom organization indeed did a good job in creating such an environment. However, there was no means for them to ensure continuous improvement and integrating cultural process back for a sustained cultural integration. Failure to do so usually causes disillusionment and results in employees abandoning their integrative efforts - a serious security concern. As Hall notes change is a complex and a circular process and there is a need to continuously evaluate and reevalu-

ate how formal changes impact the informal and subsequently get institutionalized. Typically organizations stop the change management process at this juncture. Majority of security breaches however occur post implementation of the technical edifice. There typically is another set of redefinition of formal structures following a technical implementation, and many failures become obvious at this point.

3. *Organizational stability relies on having well defined formal and informal group boundaries thus reducing friction and confusion.*

As discussed before, a major concern is the scope of change and how such changes affect stakeholder groups and current boundaries. By clearly defining roles and responsibilities, management can reduce animosity among stakeholders and streamline business processes to achieve maximum project benefit. Understanding formal and informal business processes is critical to an organization's ability to create new opportunities through project development. Any rancor and conflict because of such issues can be a cause of significant concern. Institutions that are unable to clearly demarcate the formal and informal boundaries typically result in confusing the roles and responsibilities see [1]. In our case study organization a lack of clarity of business processes, formal and informal spaces created issues related to 'social obligations' and 'responsibilities' that go beyond the law of the letter. Typically such environments can be excellent candidates for social engineering attacks and manipulations.

4. *Balancing the informal, formal and technical controls is essential to prevent over-engineered solutions.*

It goes without saying that a technical solutions to mergers and management of security are essential. Simply implementing a customer relationship system and hoping that communication needs can be addressed is not sufficient. What is required is linking technical solutions to the formal rules and obligations of various stakeholders. This necessitates the need for formal structures that support the technical edifice. Managing security after all is a holistic activity and there is a need to maintain integrity amongst the formal and the technical components. Finally the more pragmatic and normative aspects need to be evaluated as well. Ongoing education and training programs form the basis for building a security culture and a common belief system.

## 4 Conclusion

In this paper we presented the cultural analysis of two organizations undergoing merger and identified the impact of such transformations on the pertinent information security culture. We used E.T. Hall's [4] theory of silent messages to interpret the impact of radical organizational transformation on information security. The analysis allowed us to define the principles of information security in the context of organization transformations. We believe that these principle set the ground for further theorizing about culture and information security. These principle could also help practitioners to plan for information security management during such transformations.

## References

1. Backhouse, J., Dhillon, G.: Structures of responsibility and security of information systems. European Journal of Information Systems. 5(1), 2-9 (1996)
2. Dhillon, G.: Managing information system security. London: Macmillan (1997).
3. Giddens, A.: The consequence of modernity. Stanford, CA: Stanford University Press (1990)
4. Hall E. T.: The silent language (2nd ed.). Anchor Books, New York (1959)
5. Helokunnas, T., Kuusisto, R.: Information security culture in a value net. In: Engineering Management Conference, IEMC'03 on Managing Technologically Driven Organizations: The Human Side of Innovation and Change, pp. 190-194.. IEEE Press, New York (2003)
6. Ramachandran, S., Rao, V. S. C., Goles, T., Dhillon, G.: Variations in Information Security Cultures across Professions: A Qualitative Study. Communications of the Association for Information Systems. 33, 163–204 (2013)
7. Ruighaver, A.B., Maynard, S.B., Chang, S.: Organizational Security Culture: Extending the End-user Perspective. Computers & Security. 26, 56–62 (2007)
8. Segev, A., Porra, J., Roldan, M.: Internet security and the case of Bank of America. Communications of the ACM. 41(10), 81-87 (1998)
9. Von Solms, B.: Information Security—The Third Wave? Computers & Security. 19, 615–620 (2000)
10. Vroom, C., Von Solms, R.: Towards Information Security Behavioral Compliance. Computers & Security. 23, 191–198 (2004)
11. Walsham G.: Interpreting information systems in organizations. John Wiley & Sons, Chichester (1993)