Information security policies and value conflict in multinational companies

Abstract

Purpose - The purpose of this paper is to examine challenges multinational companies face during the diffusion of their information security policies. Parent companies use these policies as their discourse for legitimization of their practices in subsidiaries, which leads to value conflicts in subsidiaries. The authors postulate that, when properly crafted, information security policies can also be used to reduce the very conflicts they are creating.

Design/methodology/approach - The proposed framework is conceptualized based on the review of literatures on multinational companies, information security policies, and value conflict.

Findings - The authors identified three factors that may lead to value conflict in subsidiary companies; cultural distance, institutional distance, and stickiness of knowledge. They offer three recommendations to reduce value conflict; organizational discourse, ambidexterity, and resource allocation.

Research implications - The authors postulate that information security policies are the sources of value conflict in subsidiary companies. Yet, when crafted properly, these policies can also offer solutions to minimize value conflict.

Practical implications - The proposed framework can be used to increase policy diffusion success, minimize value conflict, and in turn, decrease information security risk.

Originality/value – The growing literature on information security policy literature has yet to examine the diffusion of policies within multinational companies. The authors argue that information security policies are the source of, and solution to, value conflict in multinational companies.

Keywords - Information security, Cultural distance, Institutional distance, Stickiness, Value conflict, Organizational discourse

Paper type - Conceptual paper

1. Introduction

With the increasing number of security breaches, one of the main concerns of organizations is to ensure availability, integrity, and confidentiality of their systems and data. Organizations can use a variety of security policies to create an effective infrastructure and governance to reduce potential security breaches. Although a rich body of literature examines various aspects of security policies in organizations, information systems scholars have not paid the necessary attention from the cross-cultural perspective (Ford et al., 2003). In fact, research on cross-cultural information security is considered as one of the most important future directions in the security literature (Crossler et al., 2013).

In this paper, we focus our attention on this mostly neglected intersection of information security policies and culture research. More specifically, we aim to examine the challenges of enforcing security policies from parent companies to subsidiaries in a multinational company (MNC) context. The nature of multinational companies (MNCs) adds a layer of complexity to enforcing security policies, given cultural and organizational differences between parent and subsidiary companies. For instance, Abdul-Gader (1997) illustrated how the misconceptions of understanding about fate in the Islamic context and the technical capability of the Arab language are some of the issues that need to be considered by MNCs in Arab Gulf countries.

One of the main benefits of successful diffusion of security policies is reducing the security breach risk of MNCs. Although MNCs can span across continents, the interconnectedness of information technology emphasizes the importance of enforcing security policies on subsidiaries. For instance, after a security breach or compromise of access rights at a subsidiary company, hackers can attack the parent company through privilege escalation or social engineering. However, when parent companies use policies as discourse to legitimize their practices, they create value pluralism either directly by imposing new values or indirectly by creating institutional pluralism. In the existence of value pluralism, organizational members are forced to consider the alternative or conflicting values in their routine decision-making process. This, in turn, decreases policy diffusion success and increases the risk of security breaches. What makes the diffusion of security policies different from the previously well-established research on MNCs and legitimization literature is the twofold change security policies bring; change in routines and change in technology. In other words, successful diffusion of security policies requires not only successful policy diffusion but also successful technology diffusion.

Our goal is to make a unique contribution to the information security literature by highlighting potential issues during security policy diffusion within a MNC context and by providing recommendations to minimize value conflict resulting from this process. First, we discuss how information security policies can create value pluralism and institutional pluralism due to cultural and institutional distance between the parent company and its subsidiaries, and also due to the stickiness of security knowledge. Then we postulate that using security policies for discursive strategies, ambidexterity, and resource allocation can effectively decrease value conflict. In an essence, we emphasize that security policies should not only address the technical side of security but also provide solution for addressing potential value conflicts as individuals interpret these policies, especially in different cultural and institutional settings.

2. Related literature

2.1. Multinational companies

MNCs face various external and internal pressures. Externally, they have to consider the institutional, cultural, and economic environments of multiple countries, and they have to be isomorphic with the local institutional environment to maintain their legitimacy (Kostova and Roth, 2002). Internally, they have to create consistency among their subsidiaries by leveraging activities worldwide to retain their competitive advantages (Kostova and Roth, 2002). One strategy for MNCs to create competitive advantage is effectively sharing organizational practices (Jensen and Szulanski, 2004). MNCs can develop knowledge in one location and exploit it in another location through internal transfer of knowledge (Minbaeva et al., 2003). Considering that organizational know-how is an important part of a MNC's global integration strategy, its competitive advantage partly resides in the effectiveness of sharing these practices and routines. These practices represent the core competencies and shared values of the parent company and consists of written rules and accompanying cognitive elements (Kostova, 1999). Kostova (1999) argued that transferring these practices involves two stages: implementation and internalization. This two-stage approach highlights that diffusion of practices involves not just the adoption of the rules and routines at the organizational/structure level but also involves the acceptance of these at the individual/agency level. Internalization stage is where individuals attach value and meaning to the practice (Kostova, 1999), and thus where the potential value conflict arises.

2.2. Information security policies

The main goal of information security policies is to provide a set of rules and guidelines to protect the organization from security breaches. Under the umbrella of this goal, organizations can have variety of security policies addressing different issues such as identification and authorization, Internet access, contingency planning, and even social media use. One of the biggest challenges of organizations is employees' compliance to these security policies. A majority of the existing studies have focused on deterrence and control based factors to investigate employees' compliance with security policies. These factors include the use of sanctions (Bulgurcu et al., 2010), perception of mandatoriness (Boss et al., 2009), fear appeals (Boss et al., 2015), moral beliefs (Vance and Siponen 2012), and security related stress (D'Arcy et al., 2014).

However, studies in an alternative research stream argue that merely exerting power on employees may not be effective in substantiating security policies, and propose understanding and identifying users' values as the first step of implementing rules (Kolkowska, 2005; Kolkowska and Dhillon, 2013). In other words, organizations may have better success in implementing security policies by motivating employees, raising awareness, and providing rewards. For example, Hedström et al. (2011) reported that the alignment of values of management and employees may yield better IS policy compliance. Furthermore, when non-compliance happens, analyzing users' underlying rationale is critical in understanding their non-compliance behaviors (Hedström et al., 2013). Compared to traditional control-based compliance

models, value-based compliance models involve employees into the IS policy design and implementation process, and emphasize on how the implementation of IS policy influences employees' values (Kolkowska and Dhillon, 2013; Cram et al., 2017). This method is especially useful in the existence of various subcultures and potential value conflicts in the organization (Kolkowska, 2011).

From the MNC's perspective, while transferring the actual security policies consists of a simple process of sending the policies to the subsidiary companies, it is the implications of adhering to the requirements of such policies that create the difficulties in enforcing them. Security policies have unique features that separate them from other management practices. For instance, where a human resources practice focuses on recruiting, compensation, or performance appraisal, security policies outline the configuration of intrusion detection systems, management of cryptography keys, or designing secure infrastructure. Thus, in addition to common difficulties due to differences in norms, ethics, and values, the technical requirements embedded in security policies create unique challenges in transferring and enforcing these policies to subsidiaries. Moreover, when a parent company requires the use of a new technology in subsidiaries, it is likely that the technology will be evaluated within the social context of the subsidiary (Robey and Rodriguez-Diaz, 1989).

2.3. Value conflict

Values are defined as "concepts or beliefs about desirable end states or behaviors, that transcend specific situations, guide selection or evaluation of behavior and events, and are ordered by relative importance" (Schwartz and Bilsky, 1987, p. 551). Rokeach (1973) grouped values into terminal and instrumental values. While terminal values are defined as end-states of existence (e.g., happiness, freedom), instrumental values are defined as modes of behavior to arrive at certain end-states (e.g., capability, obedience) (Glover et al., 1997). Instrumental values are further grouped into moral based values (e.g., fairness, concern for others) and competence based values (e.g., honesty/integrity, achievement) (Glover et al., 1997).

One of the research streams in the value literature investigates the individual-organization fit (Kristof, 1996). These studies postulate that individuals tend to join organizations where they feel a positive fit between their personal values and organizational values. Thus, one can assume that, in ideal cases, there is a certain level of value congruence between individuals and their organization. In the existence of value congruence, individuals are more likely to follow 'scripted' behavior and make rational decisions (Liedtka, 1989).

It is when there is a conflict between individual values and organizational values that individuals go off script and make judgment calls case by case. During these times, they are less sure of their stand on issues, especially when conflicting values are considered equally important (Tetlock, 1986). Low levels of congruence, or higher levels of value conflict, results in increased turnover and decreased job satisfaction (Verquer et al., 2003), as well as unfavorable work attitudes and beliefs about the ethical practices of one's firm (Posner and Schmidt, 1993). Individuals in such psychological state may intentionally or unintentionally conduct behavior that can expose their

organization to security breaches. Moreover, the effectiveness of existing control-based security measures is compromised in the existence of conflicting values (Hedström et al., 2011). Therefore, while it is important to minimize value conflict for the benefit of the individual, it is also important for the benefit of the organization from the security risk perspective.

Figure 1 presents our proposed framework. Based on the extant MNC literature, we identify three factors that may create value conflict during the diffusion of security policies; cultural, institutional, and technological. These factors cause value conflict in subsidiaries, either directly through introducing new values to the organizational setting and causing value pluralism or indirectly through introducing new organizational norms, thus, causing intuitional pluralism which may lead to introduction of new values. However, parent companies can also use security policies to reduce the very conflict they are creating. We provide three recommendations to achieve this; using discursive strategies, creating ambidexterity, and allocating necessary resources. In the following two sections, we discuss our framework in detail.

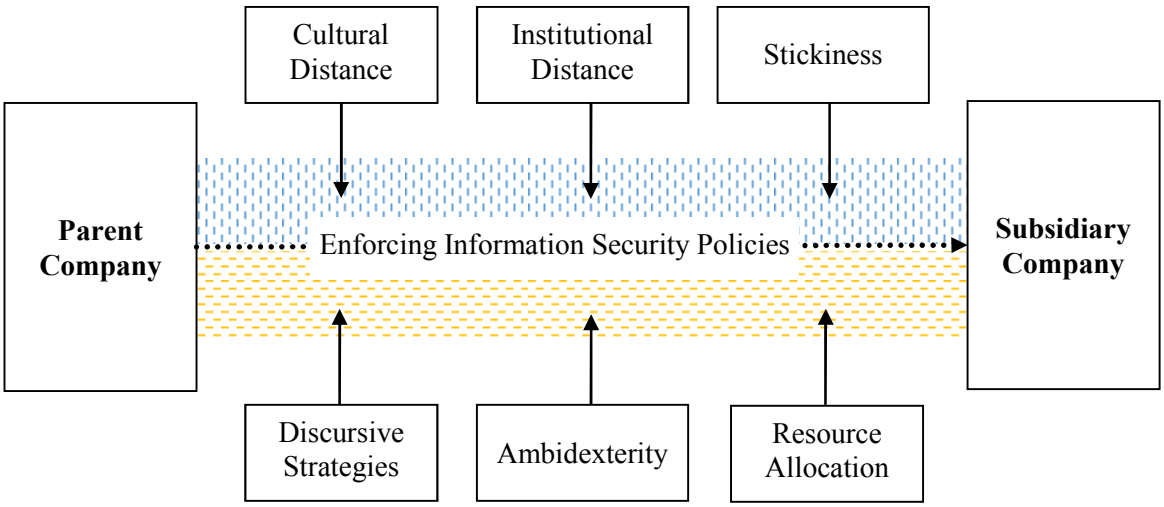

Figure 1. The proposed framework for enforcing information security policies in MNCs.

3. Information security policies as a source of value conflict

3.1. National culture and cultural distance

Various cross-cultural studies report that there is a certain level of cultural coherence within the majority of nations (Hofstede and Peterson, 2000). The concepts that describe a nation's culture can be derived from Hofstede's studies across forty nations (Hofstede, 2001). The proposed four culture dimensions from his study are power distance, individualism versus collectivism, masculinity versus femininity, and uncertainty avoidance. The cultural distance is a composite index derived from these culture dimensions and widely used in the literature (e.g., Kogut and Singh, 1988; Liu, 2004), highlighting the central role of culture in MNCs' global strategy.

The cultural dimensions have substantial importance in the success of enforcing security policies from the parent company to its subsidiaries as well. From the power distance perspective, it is important to look at the effects of restrictions that security policies bring to an organization. Access controls, for example, can be considered as an effective measure that is enforced by certain security policies. These controls restrict users from series of actions such as downloading files from the Internet, installing programs, and accessing certain parts of a computer network (Barman, 2002; Kabay, 2002). With respect to enforcing security policies, these restrictions may be problematic in high power distance cultures because adoption of power reducing technologies would be limited in such cultures (Straub et al., 1997).

Hofstede (2001) posited that masculine societies focus on careers more, which makes these societies performance oriented. Therefore, any technology or policy based change that may hinder performance would create conflicts in masculine societies. Technologies outlined in security policies such as firewalls, antivirus programs, and password protection are generally considered as having negative effect on performance (Barman, 2004). Thus, enforcing security policies in masculine societies may have certain drawbacks.

Moreover, security policies reduce ambiguity by outlining certain rules and procedures. The salience of these policies depends on the society's level of uncertainty avoidance. Weak uncertainty avoidance societies are in favor of less formalization and standardization, whereas in strong uncertainty avoidance societies, there is an emotional need for rules (Hofstede, 1997). Therefore, this cultural dimension also has a potential to inhibit the diffusion of security policies to subsidiaries.

Furthermore, security policies may require actions such as monitoring e-mail messages, recording keystrokes, and collecting private data. Similarly, these policies may outline the procedures for disciplining computer abusers in organizations (Barman, 2002). The tolerance level for these issues may differ across societies with respect to the individualism/collectivism dimension. Considering that cultural distance index captures the effects of all four cultural dimensions, MNCs that have big differences in this index compared to their subsidiaries would require different approaches in enforcing security policies.

Despite their usefulness, these culture dimensions provide only limited detail (Hofstede, 2001). For example, gross national product often matters more than national culture in the national difference context. Dewan et al. (2004) demonstrated the importance of digital divide on cross-cultural IT penetration. Similarly, Checchi et al. (2003) posited that governments play a central role in the implementation of IT policies. In another study, Ehikhamenor (2002) showed that some of the important factors that inhibit the application of information and communication technologies in Nigeria are inflation, low gross domestic product (GDP), and exchange rates.

Enforcing security policies in subsidiaries located in less developed countries would be problematic in terms of meeting the requirements of such policies. One problem is the availability of skilled IT staff. Organizations in less developed countries may not have enough human resources or capital to train their IT staff to meet the requirements. Another problem is

the availability of the necessary technology. For instance, policies may require hardware and software products that may not be available in less developed countries.

3.2. Institutional theory and institutional distance

Institutional theory considers the institutional environment as the key determinant of an organization's structure and behavior. Scott (1995) defined the three pillars of institutional theory as regulative pillar - the rules and laws to ensure stability of societies, normative pillar - the similarities between the value creation of organizations and the societal values, and cognitive pillar - the degree of consistency between organizations and existing structures of the society (Kostova and Zaheer, 1999; Busenitz et al., 2000). Based on these dimensions, Kostova (1999) developed the institutional distance construct, which captures the extent of dissimilarities between host and home organizations among these three dimensions.

The institutional distance can be considered as an alternative explanation of MNC behavior to the cultural distance. Kostova and Zaheer (1999) argued that when the institutional distance is big, it is more difficult for the MNC to establish and maintain its legitimacy in the host country. This stream of research is critical from MNCs' perspective since these companies feel pressure from two different sides: global integration and local orientation (Westney, 1983). This dual pressure is also discussed by Rosenzweig and Singh (1991) as the subsidiaries of a multinational enterprise try to keep the isomorphism with their local environments and at the same time keep the internal consistency within the enterprise.

Information systems scholars have considered these institutional factors as well. Hsu et al. (2015) highlighted the importance of recognizing, understanding, and managing institutional forces in the diffusion of cross-cultural interorganizational information systems. Similarly, Munir (2002) discussed the normative and cognitive factors within the technology transfer context. Overall, security policies have to fit into the existing institutional character of the organizations in order to be successfully enforced. Since these policies outline several practices such as disciplining computer abusers, participation in formal training and awareness programs, regular third party audits, and several new hardware and software implementations (Barman, 2002; Siponnen, 2000; Thomson and von Solms, 1998), a misfit between subsidiaries' institutional environment and requirements of the parent company's security policies will be problematic. Similar to these arguments, Hu et al. (2007) reported the effect of all three institutional forces on the initiatives to implement information systems security practices and protocols in MNCs.

3.3. Stickiness and knowledge transfer process

During the knowledge transfer process, companies recreate their complex and ambiguous routines in new settings. Ko et al. (2005) reported that the direct effects of the source's and recipient's intrinsic motivations, source credibility, and indirect effects of communication encoding and decoding competence are important determinants of the knowledge transfer. However, the stickiness of organizational practices increases the difficulties of the transfer

process (Szulanski,1996). Major sources of stickiness are the lack of absorptive capacity of the recipient, causal ambiguity, and the arduous relationship between the source and the recipient (Szulanski, 1996).

In the context of information security, the effect of stickiness will be most visible on the technological requirements of security policies. Configurations of hardware and software programs for large scale networks require advanced knowledge and experience. This type of knowledge is considered tacit and therefore hard to document, replicate, or transfer. Moreover, the slightly different configurations of computers may prevent adaptation of the same solution in different computer networks. Considering this "local" solution issue and the tacitness of information security context, transferring security policies from one organization to another would be considered as sticky.

Table 1 summarizes how aforementioned factors can potentially create value conflict during the diffusion of security policies. We postulate that these factors may conflict with the competence and moral based values of individuals; the two instrumental values identified by Rokeach (1973). Security policies are initially designed to be implemented in the parent company. Later, most MNCs use the same or direct translation of these policies in their subsidiaries. When parent companies require subsidiaries to adhere with their own security policies, value conflicts can arise due to various reasons. For instance, the implementation of employee monitoring software can create moral based value conflict due to personal values based on cultural factors as outlined in Table 1. On the other hand, lack of a particular technology in the subsidiary would prevent them from implementing it. In this case, despite their willingness and desire, employees may fail to comply with policy requirements, leading to competence based value conflict. In an essence, value conflict arises when MNC policies create value duality as a result of the requirements of their policies. Individuals are put in a position to pick between what the MNC policy requires and what they would have done based on their existing local policy requirements and expectations of their cultural and institutional environments. While each factor may lead to value conflict as discussed, the dynamics behind their effects may differ. Each subsidiary is likely to experience the effect of these factors differently based on how different they are from the parent company.

4. Information security policies as a solution to value conflict

We outline three recommendations to address the value conflict that may arise as a result of the legitimization efforts of security policies. Our first recommendation is including discursive strategies to security policies to address value conflict. Organizational discourses are not unbiased or neutral. They are used by the dominant interest groups to shape the social reality of others (Heracleous, 2004). Studies based on critical discursive analysis focus on the social construction of power relations, which makes discourses a suitable tool to investigate parent-subsidiary relationship in MNC context (Balogun et al., 2011). Similarly, Ford et al. (2008) suggested using discursive legitimization of innovation for successful diffusion. Our recommendation is built on Vaara et al.'s (2006) model of discursive legitimization strategies.

	Sample requirements of information security policies	Potential issue
Cultural factors		
Power distance	Access control to certain files	In high power distance cultures, it is harder for IT employees to limit managers' rights.
Uncertainty avoidance	Regular security audits	Subsidiaries that are in low uncertainty cultures can have harder time to comply with rigid requirements of the parent company.
Masculinity/ Femininity	Use of anti-virus software	Adoption of performance hindering software can be problematic in high masculinity cultures due to their focus on career advancement.
Individualism/ Collectivism	Use of computer monitoring	Monitoring employee behavior can result in negative effect on employee morale, satisfaction, and performance in subsidiaries that reside in individualistic cultures.
National economy		
	Implementation of advanced hardware or software	Availability of hardware and localization of software can be limited for subsidiaries that reside in developing or undeveloped countries.
Institutional factors		
Regulative	Certain level of encryption required for storing confidential information	Countries of the subsidiaries can lack the regulations that exist in the parent company's country.
Normative	Security certification	Lack of availability of certain certifications or institutions in subsidiaries' countries can limit subsidiaries to conform with normative factors.
Cognitive	Skilled employee	Lack of education in computer science and related fields in the subsidiaries' country can limit the efforts to comply with the requirements of the security policy.
Stickiness		
	Security of wireless infrastructure	Designing a secure and reliable wireless network requires unique considerations such as interference from the environment, size and shape of the buildings, etc. Due to these localized differences, achieving success using the same solution can be limited.

Table 1. Factors that may inhibit MNCs' efforts to enforce security policies to their subsidiaries.

They outlined five strategies; “normalization” to exemplify normal behavior, “authorization” to authorize claims, “rationalization” to provide rationale, “moralization” to provide the moral basis, and “narrativization” to provide a narrative structure. These strategies intertwine and can be used together to pursue the legitimization effort (Vaara et al., 2006).

For instance, for value conflicts resulting from high power distance, security policies can include authorization discourse that gives power and authority to IT employees to restrict higher level executives’ access rights. This ensures that security policies provide a discourse that outlines a new power distribution for IT tasks and routines. Similarly, a normalization discourse can be included in security policies if these policies are bringing significant changes to existing routines. For instance, when security audits are planned to be regularly conducted or when the use of security tools such as anti-virus, content filter, or two-factor authentication is planned to be implemented, security policies can be a source that explains this new norm. Both rationalization and normalization discourses can provide the necessary momentum to shift individuals’ cognitive maps to create new mental frames. When policies require changes that are closely associated with ethics and privacy, such as data sharing or monitoring of computer use, network activity, and emails, moralization discourse can be an effective strategy to prevent potential conflicts. Narrativization of the required change can also be used in conjunction with other discourses to provide further justification.

Our second recommendation is that security policies should provide alternative solutions to increase ambidexterity of the parent company. Studies illustrate that conflicting values can coexist in the same organization (Faure and Fang, 2008; Ramesh et al., 2017). But addressing this institutional pluralism requires mutual adjustment of logics. One approach to enable this coexistence is through ambidexterity of the organization (Ramesh et al., 2017). Ambidexterity is an organization’s capacity to respond to conflicting demands. Studies in the literature identify two types of ambidexterity; structural and contextual. While structural ambidexterity provides dual structures (e.g., creation of new business units) to address conflicting requirements, contextual ambidexterity provides behavioral capacity (e.g., providing support and trust to individuals to make their own judgement) to address conflicting requirements (Gibson and Birkinshaw, 2004).

In the case of enforcing security policies, both types of ambidexterity can be helpful when subsidiaries fail to comply with the policies due to strong institutional forces and differences in national economies. As discussed, institutional pluralism can lead to value pluralism; a task can be legal and illegal at the same time in different institutional environments. We argue that in the existence of institutional pluralism, security policies should provide alternative solutions and structure to accommodate conflicting demands to prevent competence based value conflicts. To achieve this, parent companies should consider various institutional conditions while creating their security policies. For instance, if a certain professional certification is not available in a subsidiary’s country, security policies should outline alternative solutions. Similarly, if saving confidential data outside of national borders is not allowed in a subsidiary’s country, security policies should provide alternative solutions. These alternative solutions can help create

structural and contextual ambidexterity by giving individuals more flexibility in their decision making in the presence of conflicting requirements.

Our third recommendation is giving information security policies enough power to allow resource allocation to ensure the success of policy diffusion. This is essential in case of limitations of technology and know-how in subsidiaries, and even more significant when tacit knowledge is necessary for implementing and internalizing the requirement of security policies. Lack of certain knowledge or technology can create competence based value conflict in subsidiaries. In these situations, parent companies should be able to provide the necessary resources to minimize this conflict. For instance, training programs, necessary technology, financial and technical support can be potential resources outlined in security policies. The effectiveness of resource allocation is mostly associated with the degree of integration and power that security policies have in their parent companies. We recommend that security policies should be tightly integrated to the corporate structure and outline various resource allocation strategies to ensure diffusion success. Table 2 presents a summary of our recommendations and provides an example of an application of each recommendation for a particular security policy requirement.

5. Discussion and conclusion

The main thesis of our paper is that information security policies are sources of, and solutions to, value conflict in MNCs. We postulate that these policies create value conflict when transferred from parent companies to their subsidiaries. The level of conflict is likely to increase with cultural and institutional distances between the parent and subsidiary company. Moreover, the stickiness of the information security context would exacerbate the potential of value conflict. In response to these issues, we recommend that security policies can be used to outline discursive strategies, increase ambidexterity of parent companies, and provide resource allocation in order to minimize value conflict.

As an illustration of our recommendations, we can focus on a MNC headquartered in Germany with two subsidiaries located in the Czech Republic and China. In such an organizational set-up, the legitimization of parent company's information security policies will create distinct value conflicts within each subsidiary. Table 3 presents a comparison of these countries based on the measures such as Hofstede's cultural distance (Hofstede, 2017), World Development Indicators (The World Bank, 2017), and Worldwide Governance Indicators (Kaufmann et al., 2010). The selected measures suggest that legitimization process will be more difficult in the subsidiary in China. On the other hand, because wireless network security policies have more sticky technology requirements (e.g., network design, router setup, etc.) than acceptable use policies which are more of a code of conduct in general, diffusion of the actual policy requirements will be more problematic for the subsidiary in the Czech Republic. This simplified example is based on the limited number of indicators as outlined in Table 3. More realistically, MNCs should examine these factors according to their own subsidiary countries and policy requirements, determine potential conflicts with subsidiary local conditions and existing subsidiary security

Organizational Discourse
Effect on value conflict: Can be used to address value conflicts that arise at the individual level such as conflicting beliefs, norms, and habits. *Main justification:* Organizational discourse can be used to legitimize parent company practices, norms, and values through cognitive changes and creation of new social realities. *Example of policy requirement:* Data Classification Policy – Restrict access based on least privilege principle; ▪ Discourse strategy: Authorization ▪ Goal: Clarification of roles and responsibilities to decrease value conflict in high power distance cultures ▪ Sample policy addendum: "This policy gives the authority to IT personnel to classify data as restricted, confidential, and public. IT personnel have the necessary authorization to limit access of all employees, managers, and executives based on their roles."
Ambidexterity
Effect on value conflict: Can be used to address value conflicts at the organizational level such as institutional pluralism. *Main justification:* Ambidexterity provides organizations the necessary structural and contextual flexibility to address conflicting local and parent requirements simultaneously. *Example of policy requirement*: Information Security Policy – Requirement of certain certifications for different roles; ▪ Ambidexterity: Contextual ▪ Goal: Provide an alternative contextual solution to prevent value conflicts due to normative factors ▪ Sample policy addendum: "Incident response teams should include an IT employee with at least two years of digital forensics experience and with [industry certification]. If [industry certification] is not available for a given subsidiary company, incident response teams should include an IT employee with at least 5 years of digital forensics experience or two years of experience with [alternative industry certifications]."
Resource Allocation
Effect on value conflict: Can be used to address value conflicts at the technological artifact level such as lack of technology or know-how in subsidiary companies. *Main justification:* Focusing on resource allocation enables companies to provide the necessary technology and know-how to subsidiaries to prevent especially competence-based value conflicts. *Example of policy requirement:* Access Control Policy – Use of biometrics for access control; ▪ Use of resources: Provide technology ▪ Goal: Provide the necessary resources to address value conflict as a result of lack of technology in the subsidiary's environment ▪ Sample policy addendum: "Designated areas must have fingerprint based access control. If [subsidiary company] does not have access to the technology, [parent company] will provide the necessary hardware/software to [subsidiary company]."

Table 2. Recommended approaches for using security policies to decrease value conflict in subsidiaries.

policies, and explore different opportunities to adapt their policies to the subsidiaries with minimum value conflict. To achieve this, MNCs can implement a maturity model to move all subsidiary security policies to the parent company level, starting with high value conflict and security risk issues.

Parent Company Country	Subsidiary Company Country	Security Policy	Cultural Distance	Economical Distance	Institutional Distance	Technology Stickiness
Germany	China	Acceptable Use	High	High	High	Low
Germany	Czech Republic	Wireless Network Security	Low	High	Moderate	High

Measures:
Cultural Distance: Power distance, Individualism, Masculinity, Uncertainty avoidance
Economical Distance: GDP per capita
Institutional Distance: Ease of doing business, Government effectiveness, Regulatory quality, Educational attainment
Technology Stickiness: General requirements of a given policy

Recommendations: Parent company should prioritize providing the necessary organizational discourse and contextual/structural ambidexterity for the subsidiary in China and prioritize providing the necessary resources to manage the stickiness due to the tacit knowledge required for the implementation of the wireless security policy in the subsidiary in the Czech Republic.

Table 3. Illustration of implementation of proposed recommendations for enforcing security policies to subsidiaries.

While information security and globalization can be considered as two sides of the same coin, the lack of cross-cultural studies in the information security literature, especially at the policy level, is worrisome. Our goal is to provide a framework as a starting point to fulfill this important gap. We argue that information security policies should be more than mere guidelines for technical solution. They have the power to create and eliminate value conflicts in organizations. Therefore, organizations should craft each security policy with the utmost attention to potential solutions that the policy can bring to value conflicts. The practical implications of our study are also vital. For instance, neglecting the cultural and institutional differences may result in loss of resources, high employee turnover, and even increased security breaches. Moreover, if it is not executed properly, the transfer of such policies may increase the dual pressure on the subsidiary, which in return may hinder their performance.

In our approach we suggest to use policies to prevent potential value conflicts that they are likely to create rather than to use policies to create value in MNCs. However, one can argue that carefully crafted policies lead to better overall security for MNCs and thus create value

indirectly. For instance, from the external threat perspective, given their size and resources, it is likely that parent companies have more detailed and advanced policies than their subsidiaries. When parent companies and their subsidiaries are in sync in terms of policy requirements, they are less prone to attacks from outside. Similarly, from the internal threat perspective, since value congruence is essential for employee satisfaction, it is likely that decreasing value conflict would decrease potential of insider attacks. Overall, when MNCs craft their policies with the consideration of subsidiary cultural and institutional environment as we have suggested in our framework, this will create a more security-conscious organization. In such a climate, all employees would care about security intrinsically rather than as a requirement, which may lead to better information security.

One limitation of our framework is the fact that the business context of the MNC may affect the salience of security policies. Companies in certain industries may need more security than others to protect their company specific information such as patents, source codes, manufacturing processes, etc. On the other hand, our framework opens many directions for future research. One direction can be the investigation of subsidiary absorptive capacity, which is considered as one of the most important determinants of knowledge transfer (Minbaeva et al., 2003; Szulanski, 1996). Another opportunity to take this study one step further is to investigate the effect of MNC's structure (e.g., multinational, international, global and transnational) on the diffusion process. Each structure has a different configuration of assets and capabilities, role of foreign subunits, and development and diffusion of knowledge (Kostova and Roth, 2003). In order to validate the proposed framework and conduct the suggested future studies, series of case studies can be conducted in MNCs with subsidiaries in different cultural, economic, and institutional settings.

References

Abdul-Gader, A.H. (1997), "Information systems strategies for multinational companies in Arab Gulf countries", *International Journal of Information Management*, Vol. 17 No. 1, pp. 3-12.

Balogun, J., Jarzabkowski, P. and Vaara, E. (2011), "Selling, resistance and reconciliation: A critical discursive approach to subsidiary role evolution in MNEs", *Journal of International Business Studies*, Vol. 42 No. 6, pp. 765–786.

Barman, S. (2002), *Writing Information Security Policies*, New Riders, Indianapolis, IN.

Boss, S.R., Kirsch, L.J., Angermeier, I., Shingler, R.A. and Boss, R.W. (2009), "If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security", *European Journal of Information Systems*, Vol. 18 No. 2, pp.151-164.

Boss, S.R., Galletta, D.F., Lowry, P.B., Moody, G.D. and Polak, P. (2015), "What do users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors", *MIS Quarterly,* Vol 39 No. 4, pp. 837–864.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010), "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness", *MIS quarterly*, Vol. 34 No. 3, pp.523-548.

Busenitz, L.W., Gomez, C. and Spencer, J.W. (2000), "Country institutional profiles: Unlocking entrepreneurial phenomena", *Academy of Management Journal*, Vol. 43 No. 5, pp. 994-1003.

Checchi, R.M., Po-An Hsieh, J.J. and Straub, D.W. (2003), "Public IT policies in less developed countries: a critical assessment of the literature and a reference framework", *Journal of Global Information Technology Management*, Vol. 6 No. 4, pp. 45-64.

Cram, W.A., Proudfoot, J.G. and D'Arcy, J. (2017), "Organizational information security policies: a review and research framework", *European Journal of Information Systems*, pp.1-37.

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M. and Baskerville, R. (2013), "Future directions for behavioral information security research", *Computers & Security*, Vol. 32, pp. 90–101.

D'Arcy, J., Herath, T. and Shoss, M.K. (2014), "Understanding employee responses to stressful information security requirements: a coping perspective", *Journal of Management Information Systems*, Vol. 31 No. 2, pp. 285-318.

Dewan, S., Ganley, S. and Kraemer, K.L. (2004), *Across the digital divide: a cross-country analysis of the determinants of IT penetration*, Personal Computing Industry Center, UC Irvine.

Ehikhamenor, F.A. (2002), "Socio-economic factors in the application of information and communication technologies in Nigerian print media", *Journal of the American Society for Information Science and Technology*, Vol. 53 No. 7, pp. 602-611.

Faure, G.O. and Fang, T. (2008), "Changing Chinese values: Keeping up with paradoxes", *International Business Review*, Vol. 17 No. 2, pp. 194–207.

Ford, D.P., Connelly, C.E. and Meister, D.B. (2003), "Information systems research and Hofstede's Culture's Consequences: an uneasy and incomplete partnership", *IEEE Transactions on Engineering Management*, Vol. 50 No. 1, pp. 8-25.

Ford, J.D., Ford, L.W. and D'Amelio, A. (2008), "Resistance To Change : Resistance the Rest of the Story", *The Academy of Management Review*, Vol. 33 No. 2, pp. 362–377.

Gibson, C.B., Birkinshaw, J. (2004), "The antecedents, consequences, and mediating role of organizational ambidexterity", *Academy of Management Journal*, Vol. 47 No.2, pp. 209-226.

Glover, S.H., Bumpus, M.A., Logan, J.E. and Ciesla, J.R. (1997), "Re-examining the influence of individual values on ethical decision making", *From the Universities to the Marketplace: The Business Ethics Journey*, Vol. 16 No. 12, pp. 109–119.

Hedström, K., Karlsson, F. and Kolkowska, E. (2013), "Social action theory for understanding information security non-compliance in hospitals: the importance of user rationale", *Information Management & Computer Security*, Vol. 21 No. 4, pp. 266-287.

Hedström, K., Kolkowska, E., Karlsson, F. and Allen, J.P. (2011), "Value conflicts for information security management", *Journal of Strategic Information Systems*, Vol 20. No. 4, pp. 373-384.

Heracleous, L. (2004), "Interpretivist approaches to organizational discourse", in Grant, D., Hardy, C., Oswick, C. and Putnam, L. (Eds.), *The Sage Handbook of Organizational Discourse*, SAGE Publications, London, UK, pp. 175–192.

Hofstede, G. (1997), *Cultures and Organizations: Software of the Mind*, McGraw Hill, New York, NY.

Hofstede, G. (2001), *Culture's Consequences: International Differences in Work Related Values. 2nd ed*, Sage, Thousand Oaks, Ca.

Hofstede, G. (2017), *Hofstede Insights*, available at: https://www.hofstede-insights.com.

Hofstede, G. and Peterson, M.F. (2000), "National culture and organization culture", In N. Ashkanasy, C. Wilderom, and M. F. Peterson (Eds.), *Handbook of Organizational Culture and Climate*, Sage, Thousand Oaks, CA, pp. 401-415

Hsu, C., Lin, Y.-T. and Wang, T. (2015), "A legitimacy challenge of a cross-cultural interorganizational information system", *European Journal of Information Systems*, Nature Publishing Group, Vol. 24 No. 3, pp. 278–294.

Jensen, R. and Szulanski, G. (2004), "Stickiness and the adaptation of organizational practices in cross-border knowledge transfers", *Journal of International Business Studies*, Vol. 35 No. 6, pp. 508-523.

Kabay, M.E. (2002), "Developing security policies", In S. Bosworth and M. E. Kabay (Eds.), *Computer Security Handbook. 4th ed*, John Wiley & Sons, Inc., New York, NY.

Kaufmann, D., Kraay, A. and Mastruzzi, M. (2010), "The Worldwide Governance Indicators: Methodology and Analytical Issues", *World Bank Policy Research Working Paper No. 5430*.

Ko, D., Kirsch, L.J. and King, W.R. (2005), "Antecedents of knowledge transfer from consultants to clients in enterprise system implementations", *MIS Quarterly*, Vol. 29 No. 1, pp. 59-85.

Kogut, B. and Singh, H. (1988), "The effect of national culture on the choice of entry mode", *Journal of International Business Studies*, Vol. 19 No. 3, pp. 411-431.

Kolkowska, E. (2005), "Value Sensitive approach to IS security-A socio-organizational perspective", *Proceedings of the 11th Americas Conference on Information Systems, Omaha,* pp. 3310-3317.

Kolkowska, E. (2011), "Security subcultures in an organization – exploring value conflicts", in Tuunainen, V., Nandhakumar, J., Rossi, M. and Soliman, W. (Eds), *19th European Conference on Information Systems, Helsinki*, pp. 2765-2776.

Kolkowska, E. and Dhillon, G. (2013), "Organizational power and information security rule compliance", *Computers & Security*, Vol 33, pp. 3-11.

Kostova, T. (1999), "Transnational transfer of strategic organizational practices: a contextual perspective", *Academy of Management Review,* Vol. 24 No. 2, pp. 308-324.

Kostova, T. and Roth, K. (2002), "Adoption of an organizational practice by subsidiaries of multiniational corporations: institutional and relational effects", *Academy of Management Journal*, Vol. 45 No. 1, pp. 215-233.

Kostova, T. and Roth, K. (2003), "Social capital in multinational corporations and a micro-macro model of its formulation", *Academy of Management Review*, Vol. 28 No. 2, pp. 297-317.

Kostova, T. and Zaheer, S. (1999), "Organizational legitimacy under conditions of complexity: the case of the multinational enterprise", *Academy of Management Review*, Vol. 24 No. 1, pp. 64-81.

Kristof, A.L. (1996), "Person-organization fit: an integrative review of its conceptualizations, measurement, and implications", *Personnel Psychology*, Vol. 49 No. 1, pp. 1–49.

Liedtka, J.M. (1989), "Value Congruence : The Interplay Of Individual And Organizational Value Systems", *Journal of Business Ethics*, Vol. 8 No. 10, pp. 805–815.

Liu, W. (2004), "The cross-national transfer of HRM practices in MNCs: an integrative research model", *International Journal of Manpower*, Vol. 25 No. 6, pp. 500-517.

Minbaeva, D., Pederson, T., Björkman, I., Fey, C.F. and Park, H.J. (2003), "MNC knowledge transfer, subsidiary absorptive capacity, and HRM", *Journal of International Business Studies*, Vol. 34 No. 6, pp. 586-599.

Munir, K.A. (2002), "Being different: How normative and cognitive aspects of institutional environments influence technology transfer", *Human Relations*, Vol. 55 No. 12, pp. 1403-1428.

Posner, B.Z. and Schmidt, W.H. (1993), "Values Congruence and Difference Between the Interplay of Personal and Organizational Value Systems", *Journal of Business Ethics*, Vol. 12 No. 5, pp. 341–347.

Ramesh, B., Cao, L., Kim, J., Mohan, K. and James, T.L. (2017), "Conflicts and complements between eastern cultures and agile methods: an empirical investigation", *European Journal of Information Systems*, Vol. 26 No. 2, pp. 206–235.

Robey, D. and Rodriguez-Diaz, A. (1989), "The Organizational and Cultural Context of System Implementation: Case Experience from Latin America", *Information & Management*, Vol. 17 No. 1, pp. 229–239.

Rokeach, M. (1973), *The Nature of Human Values*, Free Press, New Yok, NY.

Rosenzweig, P.M. and Singh, J.V. (1991), "Organizational environments and the multinational enterprise", *Academy of Management Review*, Vol. 16 No. 2, pp. 340-361.

Schwartz, S.H. and Bilsky, W. (1987), "Toward a universal psychological structure of human values.", *Journal of Personality and Social Psychology*, Vol. 53 No. 3, pp. 550–562.

Scott, W.R. (1995), *Institutions and Organizations*, Sage, Thousand Oaks, CA.

Straub, D., Keil, M. and Brenner, W. (1997), "Testing the technology acceptance model across cultures: a three country study", *Information and Management*, Vol. 33 No. 1, pp. 1-11.

Szulanski, G. (1996), "Exploring internal stickiness: Impediments to the transfer of best practice within the firm", *Strategic Management Journal*, Vol. 17 No. S2, pp. 27-43.

Tetlock, P.E. (1986), "A value pluralism model of ideological reasoning.", *Journal of Personality and Social Psychology*, Vol. 50 No. 4, pp. 819–827.

The World Bank (2017), *World Development Indicators*, available at: https://datacatalog.worldbank.org/dataset/world-development-indicators

Thomson, M.E. and von Solms, R. (1998), "Information security awareness: Educating our users effectively", *Information Management & Computer Security*, Vol. 6 No. 4, pp. 167-173.

Vaara, E., Tienari, J. and Laurila, J. (2006), "Pulp and paper fiction: on the discursive legitimation of global industrial restructuring", *Organization Studies*, Vol. 27 No. 6, pp. 789–810.

Vance, A. and Siponen, M.T. (2012), "IS security policy violations: a rational choice perspective", *Journal of Organizational and End User Computing*, Vol. 24 No. 1, pp. 21-41.

Verquer, M.L., Beehr, T.A. and Wagner, S.H. (2003), "A meta-analysis of relations between person-organization fit and work attitudes", *Journal of Vocational Behavior*, Vol. 63 No. 3, pp. 473–489.