Impact Assessment of Corporate Culture toward Information Security Incidents

Abdullah ALMUBARK[1], Nobutoshi HATANAKA[2].Dr, Osamu UCHIDA[3], Yukiyo IKEDA[4].Dr
Graduate School of Informatics
Tokyo University of Information Sciences
Chiba, Japan

***Abstract*— In today's world, ensuring the security of personally identifiable information is becoming more of a challenge. Many organizations protect their information assets by focusing on security breaches and increasing their expenses for security technologies; however, it is impossible to eliminate incidents and accidents simply by applying security technologies. This paper aims to identify the causes of information leaks by applying the organization theory and the statistical analysis method to assess the impact of corporate culture on information security incidents. Furthermore, the relationship between organizational objectives and social values is discussed.**

Keywords—Information security; Security incident; corporate culture

I. Introduction

Each year, new information security technologies are invented and applied in the workplace by organizations. However, information security incidents and accidents that involve the leakage of personally identifiable information have showed no signs of decline, e.g. the Dai Nippon Printing Co., Ltd., and the Benesse Holdings, Inc. leakage incidents.

It is impossible to eliminate information security incidents and accidents simply by applying additional security technologies. It is important to identify other factors that result in information security incidents and related accidents within the organization. The aspect of information security technology constitutes only a part of the factors that affect information security incidents. It is necessary to study those aspects that derive from people and organizations.

In this research, authors will assess the impact of corporate culture on information security incidents and the interrelationship between people and organizations. This research will also reveal that information security incidents are attributed to unaddressed information security vulnerabilities and the disharmony between organizational objectives and social values.

II. The Defects of Hierarchical Organization

Barnard [1] studied the strengths and weaknesses of hierarchical organizational structures. He considered the strengths of the hierarchical organizational structure were linked to the leaders' abilities and swift action, which leads organizations to success in this industrial age. On the other hand, Barnard pointed out that its shortcomings are disparities in the distribution of wages and in the honor and prestige among different positions, which lowers people's morale. He called these inequalities "the inverse function of the hierarchical organizational structure" and considered them to be a cause of scandals and accidents.

The following points ought to be considered as defects in the status systems and the hierarchical organization (the inverse function).

1. Defects in the Status System [1]

- A hierarchy, as a status system, distorts the true value of individuals.
- The circulation of the position of elites is unfairly limited; the ability of a specific person to strengthen exclusive positions becomes a problem.
- The system of distribution, such as equitable positions, functions, and responsibilities, is distorted; there is discrimination in the distribution of wages, honor and prestige based on status.

2. Defects in the Hierarchy [1]

- Administrative functions are exaggerated, and the function of ethics is hampered.
- It has an excessive symbolization function. The major issue is that the status and the true value of individuals are often confused.
- Though it is indispensable for the cohesiveness and coordination of organizations, a hierarchy reduces the resilience and adaptability of organizations.

Hierarchical structure is similar to that of the construction and civil engineering industry in which there are multiple layers of subcontractors, namely Tier 1, Tier 2 to Tier 5, where the bottom tier is comprised of self-employed craftsmen. This structural flaw constitutes an inverse function of the hierarchical organization which can trigger information security incidents. In contrast to an organizational structure involving multiple layers of subcontractors, Barnard [1] presented a "lateral organization," which refers to collaboration as a whole even without any formal upper-level organization or leaders [2]. According to Barnard [1], a lateral organization is composed of shareholders, creditors, consumers, raw material suppliers, and local governments, where subcontractors fall within the category of raw material suppliers. Furthermore, Barnard [1] emphasized that it is possible to prevent information security incidents and accidents through the practical application of lateral organization.

A. Sympathizing with Corporate Objectives and Social Values

Simon [3] argues against the productivity of this concept, which is determined by the relationship between the inputs and outputs in Taylorism. He considers that organizations can increase their value, prevent corporate incidents and scandals from occurring, and increase the loyalty of their employees to the organization only when their objectives and the social value are consonant. In the cases of Dai Nippon Printing Co., and Benesse Holdings, the information security incidents occurred due to disharmony between social values and organizational objectives in the organizational structure. At Benesse, this allowed a subcontractor's employee to copy personal information about Benesse's customers onto his smartphone and transfer this externally without any authorization.

B. Organizational Cause of Incidents

The "administrative principles" of an organization were presented by Simon [3], and relate to the challenges that organizations face when resolving incidents. By comprehensively considering the following points, it is conceivable that suggestions can be obtained for improving efficiency and preventing organizational incidents. Administrative efficiency is increased by:

1. Specializing work in a group (specialization).
2. Arranging the members in a hierarchy of authority (unity of command).
3. Limiting the span of control to small numbers of people at any level of the hierarchy (span of control).
4. Grouping employees according to their type of work (organization's characteristic).

Consideration must be given to the adverse effects of these factors since they can cause organizational incidents. Nevertheless, these factors do correlate positively with efficiency. In other words, overall business efficiency results from improvements in organizational efficiency and productivity. Considering that an organization can be a hotbed of incidents, it appears necessary to confirm not only the activities and decision making of an organization, but also the effectiveness and limitations of the hierarchy as is done in the collaboration method.

C. Similarities between Scandals and Incidents

Data on 140 Japanese organizations where information security incidents took place from 2006 to 2014 was collected through reliable Web sites in Japan and the IPA`s (Information Technology Promotion Agency) archives. These incidents were investigated using the points listed above in Section B. It was seen that similar scandals and incidents had similar causes, they arose from social values or corporate culture.

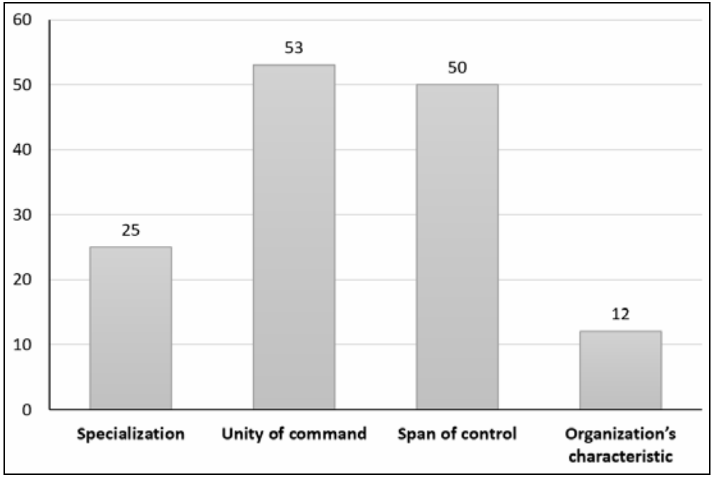

Figure 1. 140 cases of information security incidents and accidents that occurred from 2006 to 2014 were categorized using Simon's [3] suggestions..

D. Research Goals, Hypotheses and Procedure

This research identifies the defects in corporate culture that contribute to information security incidents. The goals of this paper are to:

1. Describe the impact of organizational hierarchy on corporate culture.
2. Determine the effects of corporate culture on information security incidents.

To support the determination of the effect of corporate culture on information security incidents and the development of a process through which corporate culture may be assessed, the following research hypotheses will be pursued:

- H1: Corporate culture is directly affected by the organizational hierarchy in which it is contextualized.
- NH1: Organizational hierarchy has no impact upon corporate culture.
- H2: Information security incidents and scandals are intrinsically linked to corporate culture.
- NH2: The manifestation of information security incidents and scandals is not related to corporate culture.

The research procedure was as follows:

1. Conduct a questionnaire survey concerning corporate culture.
2. Apply covariance structure analysis to extract factors of corporate culture from the survey data through an exploratory and confirmatory factor analysis
3. Induce variables concerning the organizational variable.

III. Relationship between Corporate Culture and Information Security Incidents

Hofstede [4] considers culture to be comprised of two primary elements. "Culture one" is comprised of civilization or "refinement of the mind" and encompasses elements of society and culture such as education, literature, and art. "Culture two" is a broader conception of the word and is related to the patterns of thinking, feeling, and acting that are engaged in by individuals. Individuals living and operating within the same social environment tend to share these elements. Corporate culture and incidents of organizational crime are intrinsically linked to one another, and the concepts are researched simultaneously [5]. Thus, within organizations, culture influences the perspective applied to organizational facets, including information security.

A. Organizational Culture and Misconduct

Shover [5] found that variation within the culture of an organization affects many elements of organizational performance. These include effectiveness in goal attainment in addition to criminal conduct. Generally, there is high intra-organizational cultural uniformity. Thus whether criminal or legitimate, such behaviors reinforce one another [5].

There are a variety of cultures that may be adopted within the context of an organization. The iteration of culture that is realized within an organization influences the manner in which employees interact. This influence is tangible in relation to employees' interaction with one another, and with the strategy of the organization at large. The culture of an organization varies depending upon how externally or internally oriented the culture is [6]. Culture is influential upon the behavior of employees at large given its expansive impact upon the stakeholders therein.

Hoshino [7] examined the role of corporate culture in relation to misconduct. Increasing incidents of corporate misconduct have made compliance management increasingly important within the scope of organizations. Despite such efforts, it is largely impossible to eliminate inter-organizational misconduct altogether, and thus efforts beyond merely establishing rules are essential. Moral leadership, trust among coworkers, the adoption of a pay-for-performance system, and factionalism result in superior compliance to conduct rules. Direct efforts to achieve compliance management were found to be largely ineffective, which emphasizes the importance of intra-organizational efforts to support a culture without misconduct [7]. Compliance management is directly linked to information security in the modern environment of business given that information is a basic commodity that is crucial to the ongoing well-being of modern organizations [8].

Da Veiga [9] assert that an organization's approach to information security must focus on the behavior of employees. Gebrasilase [10] state that information security culture is comprised of a set of information security characteristics that are valued by the entirety of the organization. This emphasizes the importance of culture within the organization.

Alfawaz [11] noted the difficulty in understanding the complex dynamic and uncertain characteristics related to organizational employees who perform information security activities, whether authorized or unauthorized. Information security management is influenced markedly by both individual and group behaviors and must be managed as such within the scope of organizations. Culture may potentially be quantified through a consideration of social-cultural factors within an organization [12].

The modern organizational culture is becoming increasingly dependent on information technology. Therefore, organizations must invest in the protection of their information assets. There are many processes that are essential to establish and reinforce the protection of information assets, although the most important is human cooperated behavior [8]. Culture can provide significant value for an organization. A corporate culture that focuses on information security is less likely to engage in misbehavior or harmful interaction with information assets [9].

Van Niekerk [8] researched information asset security found humans to be the greatest threat to information security. Whether due to negligence or intentional action, employees are the greatest threat to information security, oftentimes due to lack of knowledge. Thus, it is essential that organizations endeavor to establish a culture of information security so that the human factors that generate risk involved in information security are minimized and managed; however, the accomplishment of this goal is not simple [11].

B. Information Security Strategy

Within the modern environment of business, industry experts have increasingly been demanding a stronger focus on information security. Information security must be incorporated into organizational strategies to be effectively addressed; however, despite the importance, there is no clear blueprint through which a firm may achieve a culture that supports organizational culture [13]. The values that are associated with organizational culture are manifested in the practices and activities within the organization in relation to information security management [11].

Focusing on information security within organizations is a comprehensive process. Kayworth [13] conducted qualitative research comprised of interviewing 21 information security executives from 11 organizations and found that information security strategies are complex. Generally, these strategies are comprised of a strategically focused information strategy that incorporates not only IT products and solutions but also social alignment mechanisms and organizational integration mechanisms. These strategies are often managed through the institution of a control-based compliance model [14].

C. Quantifying Information Security in the Workplace

The mitigation of information security threats depends on the determination of the source of threats. Often, such threats stem from organizational insiders. Insiders are capable of causing greater damage due to their position; thus, they must be identified and subsequently targeted by countermeasures. Information security countermeasure strategies are a means of addressing particular threats [15]. The socio-technical approach is a means to achieve three objectives: achieving a balance between security essentials and the need to enable the business, maintaining compliance, and ensuring that the strategy is appropriate for the organizational culture [13].

Employees are central to the protection of organizational information, which has prompted the study of what researchers have coined "security culture." By embedding security culture into the corporate culture, employee behaviors that protect the information of the organization is positively influenced [16]. Employee compliance is one of the more difficult facets of information security measures, which highlights the importance of enforcement, and one facet is monitoring. One way to directly control and observe employee behavior in relation to information security is by monitoring employee computers [17].

To measure employee behavior related to information security, Padayachee [18] studied the extrinsic and intrinsic motivations that influenced employees' propensity related to compliant information security behavior. Employee behavior in this regard is comprised of a set of core information security activities that must be adhered to by end-users to promote security.

Information security within organizations is also affected by social media. Social media provides both opportunities and risk for organizations, underlining the importance of effectively managing all facets of electronic information within the organization [19]. Talib [20] have found that information security within the organization must be complemented by further research into how technology is used by employees. By focusing on overall information security behaviors, an all-around information security culture may be established that is present within both the home and office environment [20].

Alnatheer [21] endeavored to develop a measurement of information security culture. The purpose of this research was in recognition of the apparent lack of a clear conceptualization of information security culture, and the factors that constitute and influence the culture. To facilitate this, 8 interviews were conducted with information security experts. It was found that security culture is in effect a reflection of security awareness and security ownership within the organization [21]. Dzazli [22] determined the basic factors involved in information security management systems in order to determine their quality. It was found that there are a number of underlying dimensions of social factors, although technical factors are fewer. This indicates the importance of individual perception and risk management efforts undertaken.

IV. ORGANIZATIONAL ELEMENTS

Among the methods of corporate organization, there is the approach to an organization's exterior based on its form (the hard way of perceiving an organization: form, structure, etc.) and the approach to an organization's interior (the soft way of perceiving an organization: culture, values, etc.). One of the methods, which focuses on systems that are composed of people and organizations, applies the complex adaptive system approach emphasized by Robert [23] to organizations and clarifies both the development of corporate culture and the process of forming corporate values. In the organizational theory, the agent is regarded as "one that makes independent judgments and adaptively changes," and people are regarded as a type of agent.

The organization is composed of four elements: agents, organizational objectives, relationships between agents, and management. This way of thinking, in which managers are themselves mere agents, argues that managers are the same as employees in relation to agents. If the policies or objectives of managers are not appropriate, feedback is carried out regarding their appropriateness, and such policies or objectives are then amended. There are cases in which employees accept inappropriate policies or objectives without changing them. In such cases, there is the problem of whether managers or employees have somehow reacted to inappropriate policies with particular values. In the approach to an organization's interior, even in the case of managers, the only factor that exists is the mutual relationship between managers and employees.

In addition, though managers are normally considered to be in possession of authority or power, it is merely a false appearance; employee agents are the ones who control on-site location information, persons, money, and facilities. Without interaction with the employee agents, manager agents would not be able to achieve the goals that they set. Conversely, when managers are demonstrating clear management objectives and the importance of social compliance, it is on this basis that the corporate culture is developed through a mutual relationship between agents, and employees react to the importance of corporate values.

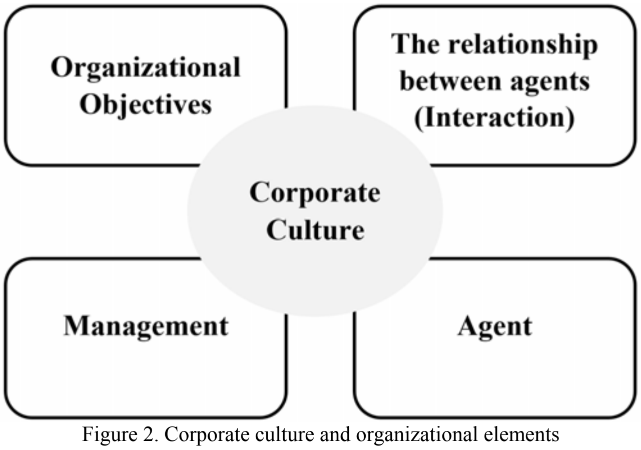
Organizational Objectives
The relationship between agents (Interaction)
Corporate Culture
Management
Agent

Figure 2. Corporate culture and organizational elements

V. ASSESSMENT OF CORPORATE CULTURE

The corporate culture impact assessment is defined as "any change to the corporate culture, whether adverse or beneficial, wholly or partially resulting from" a corporate culture aspect, which is similar to the ecological impact assessment and the privacy impact assessment [24]. In addition, the corporate culture aspect is "the element of an organization's activities that can interact with" the corporate culture, as noted in section (IV); these elements include agents, objectives, management, and interaction between agents.

When seeking to determine the level of information security of a company, the essential first step is assessing its corporate culture. When an organization has experienced a security problem, the importance of this assessment is magnified. In the absence of a new strategic goal or a problem that must be overcome, "culture analysis turns out to be boring and often fruitless. The potential insights that culture can bring you will only occur when you discover that some problem you are trying to solve or some change that you are trying to make depend very much on cultural forces" [6].

Within the context of cultural changes and assessments, the diversity that is inherent within a culture must be taken into account. Culture is not always a single entity that influences the workplace in one way or another. Rather, culture is comprised of a variety of individual segments, each of which may have an influence upon an intended organizational change or strategic initiative. Some elements of a culture may be supportive of a change, while others may inhibit it. It is important to conduct a comprehensive assessment of an organization to determine the elements of its culture that will support a proposed change and those elements that will cause resistance. Any cultural aspects that may hinder the change can then be addressed [6].

When performing such an assessment, it is important to take into account the methods used for measurement. Many tools are available that can assist managers with achieving their assessment goals. One of these tools is the survey. Surveys that measure the dimensions of culture are helpful when seeking to quantify the iteration and levels of the culture [6]. However, surveys that generate data derived directly from members of the community must be viewed with skepticism given the intimate relationship of those being surveyed with the information being collected. It is important that the researcher take into account any individual bias that employees may have in relation to answering survey questions honestly. They may be afraid that any negative responses will reflect poorly upon them, so they may have little motivation to respond honestly to the survey.

A. Types of assessment

Schein [6] explored a cultural assessment instrument that divides culture into four types, each with varying levels of internal and external orientation. The "clan" type of culture is characterized by flexibility and an internal orientation. The "hierarchy" form of culture is stable and oriented internally. The "market" culture is externally oriented and noted for its stability. Finally, "adhocracy" is a culture that is both flexible and externally oriented [6]. The type of culture that is in place within an organization will influence the efficacy of measures used to address problems or to successfully implement change.

An additional assessment tool explored by Schein [6] determines the level of sociability and solidarity within the context of an organization's culture. Four cultural types emerge through this particular survey. The first is that of "networked," in which the culture is high in both sociability and solidarity. The "communal" culture is characterized by high sociability and low solidarity. A "mercenary" culture is low in sociability and high in solidarity, while the "fragmented" culture is low in both solidarity and sociability. According to this assessment tool, the characteristics of a workplace culture determine the level of cohesion that is in place among the employees. When endeavoring to establish a change or to adopt a new strategy, it is important that the workplace culture be supportive of such efforts through conjoined effort and communicability. This can be seen in the survey's focus upon sociability and solidarity.

Schein [25] also emphasized assessing the cultural dimensions of organizations to better facilitate organizational objectives. To this end, a 10-step intervention was proposed. The purpose of the intervention was to "enabling members of the organization to identify important cultural assumptions and to evaluate the degree to which those assumptions aid or hinder some changes that the organization is trying to make" [25]. As stated previously, assessments of culture are a key first step when initiating broad organizational change as they enable an appropriate strategy to be identified and tailored to it.

VI. Data and Analysis

A. Factors Influence Corporate Culture

The factors and issues related to scandals were proposed by Hoshino [7] and the research group at Hitotsubashi University; while there are existing case studies that have discussed scandals within organizations in Japan, we attempted to use these factors to explain the similarities between information incidents and scandals.

In accordance with Hoshino [7] standardize "culture of fraud and neglect of violation in the workplace" instead of the very number of occurrences of violations, organizational incidents and scandals that cannot be made into concrete measurement items without specifying the type of industry, and treat this as the dependent variable. Thus, author introduce variables as predictor variables that are operable based on management, which not only include "individual culture" but also the state of the initiative towards leadership and compliance, the strength of segregation of duties, and the degree of performance-based human resource management. In addition, competitive pressure is also introduced as a predictor variable in performance or the markets of organizations that comprise an environmental factor in which direct operation by management is not always possible. Furthermore, "sectarian behavior" as corporate culture and "trust in coworkers and managers in the workplace" are also made predictor variables. While it is difficult to make causal inferences among variables from research, it would be appropriate to consider that "culture of fraud and neglect of violation in the workplace" are influenced by "operable organizational factors depending on management", and "corporate cultures pertaining to unfairness" are themselves also influenced by "operable organizational factors depending on management". It is meaningless to explain "(illegal and violation-neglecting) cultures" with only "individual, etc. cultures", and it is important to explain them using operable organizational factors based on management.

In this research, covariance structure analysis was applied for comparisons through statistical testing of the effects of the latent variables (corporate culture type) on the observed variables.

B. Questionnaire Development and Data Collection

Based on factors and issues related to incidents and scandals were proposed by Hoshino [7]; a questionnaire for the IT department of the IMAM Institute in Tokyo was developed in both Japanese and English. The distribution method was on-site at the institute. The survey consisted of two parts. Part one gathered information on employee demographics using multiple choice questions, allowing the researcher to examine such factors as the age of the department, job duties, and background of information security experience. In part two, 43 observed variables were classified into 8 categories as shown in Table 1.

The observed variables concerned with the section "culture of fraud and neglect of violation in the workplace" were measured on a 5-point Likert scale (1: None to 5: Frequently). And other observed variables were measured on a 5-point scale (1: Disagree to 5: Agree). This part will used for covariance structure analysis.

TABLE 2. RESPONDENT PROFILES

Participant's Answers		**100%**
Participant's age	20 or under	3
	21 – 30	24
	31 – 40	37
	41 – 50	31
	51 – 60	5
Participant's gender	Male	81
	Female	19
Job duties	Leader	1
	Manager	2
	Employer	91
	Contractor	6
Education level	Graduate School	48
	Collage	43
	Other	9
I have violated by a virus to my computer		78
I have looked into a password of another person		36
I have shared my password to another person		14

TABLE 1. QUESTIONNAIRE ITEMS

Culture of fraud and neglect of violation in the workplace	Did you ever disobey the basic rules in your workplace?
	Have you ever made false reports in your workplace?
	Have you seen the performance of dishonest means with respect to important decisions in the past?
	In your workplace, did your manager ever neglect the fraud even knowing them?
	In your workplace, did your manager ever instruct you to conceal the fraud?
	Do you have an atmosphere that earns a profit, even by illegal act?
	For problems such as illegal act happened in other organizations, Do you have an atmosphere that your organization would not take the same actions?
	Does an illegal act done by the group of decision making in your workplace?
Trust toward the workplace	Do you think the coworker can collaborate closely in your workplace?
	Do you think the information transfer between members is performed widely and smoothly in your workplace?
	Do you think your co-worker reliable at work?
	Do you think your manager reliable on work?
	If you put priority on doing the right thing, will your manager and co-worker support you?
Sectarian behavior	Do some people form a strong conspiracy in your workplace?
	In your workplace meeting, Do some people work together to get a favorable resolution with complicity?。
	Is it difficult for you to propose an opposite opinion against the members of mainstream faction in your workplace meeting?
	The individual who does not belong to the influential faction (good friend group), will there be disadvantage on work or will there any harassment in your workplace?
	Are there any "escape goat" (people to sacrifice) in your workplace, so that anything inconvenient can be attributed to them?
	Are the people surrounded by the yes-man subordinate leaders of your organization or workplace?
	Does the subordinate who does not do the present (gift) for the manager become disadvantageous by promotion in your workplace?
	Are the individual who actively speak sound arguments labeled as "problem child", and ignored or shunned in the workplace?
	Are the claims of some of members almost all accepted regardless of its content?
Belonging scale	In a face-to-face meeting with the opponent, it happened that you could not express your dissenting opinion.
	In a meeting, even the same proposal will have different result in being passed or not depending on the proponent.
	When trouble occurs, the atmosphere there is more of "whose responsibility it is" than of "what the cause is".
	People are evaluated more from likes and dislikes than the way they do work.
	The priority of work is often decided by who has requested.
Leadership at the workplace level	Does the top of your workplace put entrenchment in the first place instead of self-sacrifice?
	When you are confused in a judgment, will your manager give appropriate Legal instructions for the entire workplace?
	Does your manager brandish their power to the subordinate one hand, but behave obediently to people in the upper position?
	Have your manager shown enough leadership on work?
Moral leadership	In your workplace, does a manager emphasize restraint of the injustice definitely?
	Are the managers in your workplace behaving as the moral model for others?
	Have the managers in your workplace a strong sense of mission?
compliance system	Does a system to check the manager function effectively in your organization?
	Does enough information disclose it at the time of decision making in your workplace?
	Do you aim to establish a compliance (legal and ethical compliance) in your workplace?
Other single indicators	Is the regular employee in your workplace alienated except for special conditions?
	Have your employment regulations been strictly followed in workplace?
	Has the work objective of each person been clear every day?
	Do you let you reflect achievements and the result that each person achieved on the occasion of decision of the annual raise in salary, promotion in the last year directly in your organization?
	Is there fierce competition existing in the market activities in your company (organization)?
	Does your organization produced a good performance and been highly evaluated during the past decade?

C. Exploratory Factor Analysis

An exploratory factor analysis was applied to extract factors. Eight factors were extracted from the observed variables. All coefficient alpha values were more than 0.8, which indicates that observed variables were positive.

1. Culture of fraud and neglect of violation in the workplace.
   Eight question items were created with regard to how much corruption or illegal acts take place in the workplace. These eight question items showed a high single factor (0.876 contribution ratio), the coefficient α for the total number of points was high at 0.802, and it was confirmed that the factorial validity of the scale is high.

2. Trust in the workplace.
   Five question items were prepared, As a result of the factor analysis of these items, a single factor was extracted (0.875 contribution ratio), the coefficient α was high at 0.820, and it was found that the items can be used as a scale with one dimensional properties.

3. Sectarian behavior
   After comprising nine question items that conceivably measure sectarian behaviors, a single factor was extracted, the contribution ratio was extremely high at 0.906, and the coefficient α was high at 0.905.

4. Belonging scale
   The five items were used in this analysis. A single factor was extracted, the contribution ratio was 0.856, and the coefficient α was high at 0.811.

5. Moral leadership
   Though the moral leadership of management that Barnard [1] states of is a concept extended over a broad range, three question items here that are conceivably related to corruption and the neglect of violations were used to make measurements. The contribution ratio was 0.676, and the coefficient α was at 0.894.

6. Level Leadership at the workplace level
   After measuring the moral leadership of management and managers at the workplace level using four question items, the contribution ratio here was 0.718, and the coefficient α was sufficiently high as three items at 0.894.

7. Development of compliance system
   Three question items were given to measure if such organizations were aiming towards compliance management or carrying out information disclosures. The contribution ratio was 0.618, and the coefficient α was 0.827.

8. Other single-item indicators
   Items that were conceivably sufficient in attaining information with single items were used for analysis without change as single item indicators. They were specifically “employment security, “employment regulation strictness”, “segregation of duties”, “performance-based human resource management”, “market competitiveness”, and “corporate performance”. The contribution ratio was 0.862, and the coefficient α was 0.849.

Through the results of the exploratory factor analysis, variables concerned with information security incidents have been induced. The results shown in Table 3.4.5. The results indicate that all eight factors are valid for confirmatory factor analysis.

TABLE 3. SUMMARY OF EXPLORATORY FACTOR ANALYSIS

Latent Variables	Number of Questions	Contribution Ratio	Coefficient Alpha
Culture of fraud and neglect of violation	8	0.846	0.802
Trust in the workplace	5	0.875	0.820
Sectarian behavior	9	0.906	0.905
Belonging scale	5	0.856	0.811
Moral leadership	3	0.676	0.894
Leadership at the workplace level	4	0.718	0.894
Development of compliance system	3	0.618	0.827
Other single indicators	6	0.862	0.849

TABLE 4. CROSS LOADINGS OF ITEMS

	Factor							
	1	2	3	4	5	6	7	8
Compliance7	.911	.065	.026	.061	-.059	.011	-.019	-.084
Compliance6	.884	-.020	-.070	-.014	.048	.004	-.035	.055
Compliance5	.651	-.037	.017	-.077	.005	.190	.114	-.069
Trust1	.023	.826	-.029	.062	.007	-.014	-.002	-.066
Trust3	.021	.821	.015	-.004	-.010	-.070	.040	.031
Trust4	-.029	.749	-.008	-.053	.016	.081	-.016	.121
Belonging4	-.185	.055	.875	-.017	-.040	.074	.040	-.036
Belonging5	.119	.033	.850	-.015	.026	-.015	-.030	-.064
Belonging3	.049	-.135	.742	.045	.032	-.061	.018	.156
Sectarian7	-.081	-.052	-.073	.901	.024	.084	.129	-.034
Sectarian6	.113	-.010	.144	.814	-.029	-.067	-.083	.029
Sectarian2	-.020	.082	.009	.771	.041	-.008	-.067	.026
Culture_fraud3	.026	-.007	.001	-.087	.963	.033	-.057	-.014
Culture_fraud2	-.006	-.063	-.069	.117	.654	-.076	.085	.153
Culture_fraud7	-.039	.102	.095	.056	.560	.029	-.005	-.177
Moral2	.045	-.001	.006	.052	.010	.821	.117	.027
Moral3	.112	-.011	.002	-.018	-.018	.812	-.101	.122
Other3	.015	.000	.010	.034	.008	.085	.890	-.114
Other1	.196	.066	.023	-.061	-.004	-.168	.537	.234
Leadership4	-.044	.075	.025	.014	-.007	.160	-.037	.752

	Induced Variables
Culture of fraud and neglect of violation	Have you ever made false reports in your workplace?
Trust in the workplace	The information transfer between members is performed widely and smoothly.
Sectarian behavior	The subordinate who does not give a present (gift) to the manager has a disadvantage regarding promotions.
Belonging scale	When incidents or accidents occur, the concern is more of "whose responsibility it is" than of "what the cause is."
Moral leadership	The managers in my workplace behave as a moral model for others.
Leadership at the workplace level	The manager shows enough leadership at work.
Development of compliance system	I am aiming to establish a compliance (legal and ethical compliance).
Other single indicators	The work objective of each person is clear every day.

D. Result Discussion

The results of the confirmatory factor analysis were induced and are shown in Figure 3. As a result, the most influential factors are “sectarian behavior” and “belonging scale.” The more “sectarian behavior” increases, the higher “culture of fraud and neglect of violation in the workplace” rises.

Furthermore, a greater level of “moral leadership” demonstrated by the administration, in combination with an increase in “trust in the workplace,” results in lower “culture of fraud and neglect of violation”. It also shows that “other single indicators” have certain effects, but the influence is small compared to the variables mentioned above.

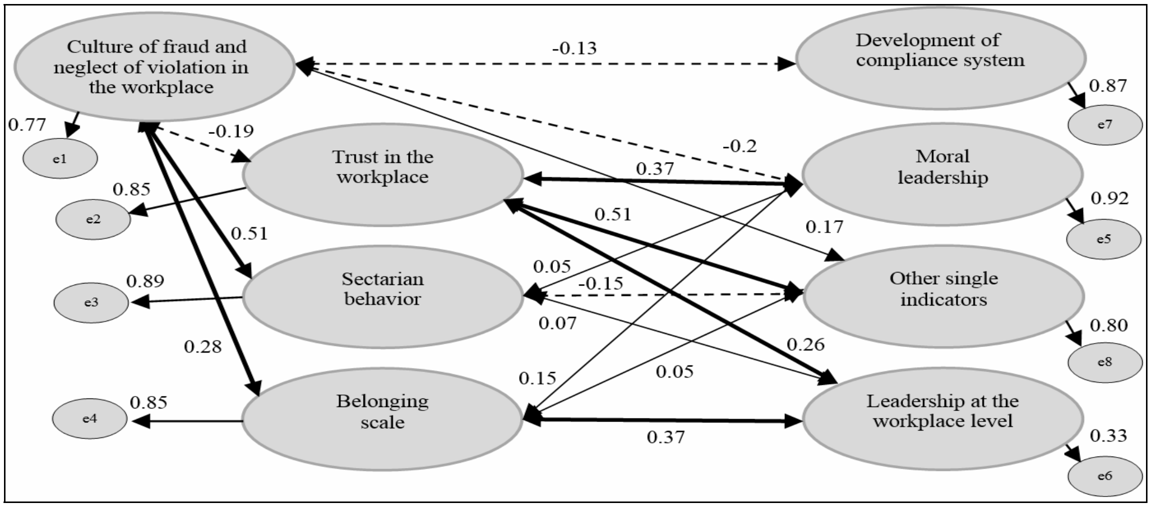

Figure 3. Result of confirmatory factor analysis (GFI= 0.915, CFI= 0.971, RMSEA = 0.035)

In addition, it has been shown that “culture of fraud and neglect of violations” decreases in organizations that score higher in “development of compliance systems.” Its influence, however, is limited. At the same time, whereas “moral leadership” is effective on the suppression of “culture of fraud and neglect of violation in the workplace”, “leadership at the workplace level” does not directly affect “culture of fraud and neglect of violations in the workplace.” However, “leadership at the level of workplace” has a significant effect on “trust in the workplace”, “sectarian behavior” and “belonging scale.”

As a result, it was found to be important that the superficial “development of compliance system”, which is carried out by top-down method, only has the limited effects on “culture of fraud and neglect of violation in the workplace”. Besides, it was shown that moral leadership by the management and trust relationship at workplace are more important than the “development of compliance system”.

This indicates that, in order to prevent from information incidents and accidents at the level of the workplace in the future, it is important how to foster the culture of the law, regulations and ethics at the level of workplace or organization members, which are not highly dependent on the degree of the development of the compliance system.

In order to maintain the social trust of the organization by preventing from information incident and accidents, and in order not to deteriorate the management environment, it is not necessary only to build the internal control system with the top-down method, but also to improve the culture of the organization or at the workplace by exerting leadership at the level of the management or the workplace.

In this analysis result, the result-oriented management often tends to foster “culture to neglect injustice and violations”. Corporations are often focusing on making short term profits for their stockholders and forcing the management to aim maximization benefits in a short term; that they behave in ways that adversely affect corporate employees, the environment, consumers, and even the long-term well-being of the organization, in addition, it increased the injustice and the unethical behaviors of organization Mitchell [28]. In order to prevent from these injustice and unethical behavior of companies; it would be insufficient if only the top-down compliance system was introduced, and it is important to engage in organizational activities at the level of the employees of the field and the workplace with a long-term perspective Mitchell [28]. As the measure to encourage it, Mitchell [28] proposed to bring about more socially responsible corporate culture.

Barnard [1] suggests that its shortcomings were disparities in the distribution of wages and honor and prestige among different positions, which lowered people's morale. The wage system has a problem in terms of labor motivation and organizational efficiency, the wage system has a problem from the viewpoint of information incidents and accidents. The management reflects the short-range results in the wage. Therefore, it is considered as diminishing the incentive for the organization members to distribute to the long-term benefits of the organization, and as the formation factor of the culture to produce injustice.

VII. Conclusion

The prevention of information security incidents within an organization has become a highly important topic. In this research, various concerns regarding corporate culture have been operationally defined using a questionnaire.

By utilizing the questionnaire data, it has been investigated how such culture at a general workplace is specified by the factors which can be operated by the management action, such as the culture in the workplace related to "trust in the workplace" and "sectarian behavior," the degree of "compliance" management, and the management actions of "moral leadership by the management."

The results of factor analysis show that sectarian behavior, including scale, moral leadership, and other single indicators, have a powerful influence on corporate culture as shown in Figure 3. The development of compliance systems has only a limited effect on the culture of fraud and neglect of violations in the workplace, and it does not have a very strong influence on corporate culture.

Through the application of this assessment, the areas of corporate culture that adversely affect information security within an organization can be identified.

References

[1] Barnard, I., The Functions of the Executive, Harvard University Press, 1938.

[2] MANO, The Meaning of the Concept of Lateral Organization in C.I.barnard's Theory, Hokkaido University Economic Studies, 39-1, June 1989.

[3] Simon, H., Administrative Behavior, The Free Press, 1945.

[4] Hofstede, G., Culture and Organizations: Software of the Mind. New York, NY: McGraw-Hill, 2010.

[5] Shover, N., & Hochstetler, A., Cultural explanation and organizational crime. Crime, Law, & Social Change, 37, p.1-18, 2002.

[6] Schein, E., H., The Corporate Culture Survival Guide. San Francisco: Jos-Bass, 2009.

[7] Hoshino, T., Arai, K., Hirano, S., & Yanagisawa, H., An empirical analysis of organizational climates of misconduct. Hitotsubashi University, 2(2): p.157-177, 2008.

[8] Van Niekerk, J. F., & Von Solms, R., Information security culture: A management perspective. Computers & Security, 29(4), p.476-486, 2010.

[9] Da Veiga, A., & Eloff, J. H., A framework and assessment instrument for information security culture. Computers & Security, 29(2), p.196-207, 2010.

[10] Gebrasilase, T., & Lessa, L. F., Information Security Culture in Public Hospitals: The Case of Hawassa Referral Hospital. The African Journal of Information Systems, 3(3), 1, 2011.

[11] Alfawaz, S., Nelson, K., & Mohannak, K., Information security culture: a behavior compliance conceptual framework. In Proceedings of the Eighth Australasian Conference on Information Security-Volume 105, p.47-55, Australian Computer Society, Inc, January 2010.

[12] Kruger, H., Drevin, L., & Steyn, T., A vocabulary test to assess information security awareness. Information Management & Computer Security, 18(5), p. 316-327, 2010.

[13] Kayworth, T., & Whitten, D., Effective information security requires a balance of social and technology factors. MIS Quarterly Executive, Vol. 9, No 3, p. 163-175, 2010.

[14] Hedström, K., Kolkowska, E., Karlsson, F., & Allen, J. P., Value conflicts for information security management. The Journal of Strategic Information Systems, 20(4), p.373-384, 2011.

[15] Coles-Kemp, L., & Theoharidou, M., Insider threat and information security management. In Insider Threats in Cyber Security p. 45-71, 2010.

[16] Lim, J. S., Ahmad, A., Chang, S., & Maynard, S., Embedding information security culture emerging concerns and challenges. PACIS 2010 Proceedings, p.43, 2010.

[17] Greene, G., & D'Arcy, J., Assessing the Impact of Security Culture and the Employee-Organization Relationship on IS Security Compliance. In 5th annual symposium on information assurance (ASIA'10) p. 1, June 2010.

[18] Padayachee, K., Taxonomy of compliant information security behavior. Computers & Security, 31(5), p. 673-680, 2012.

[19] Oehri, C., & Teufel, S., Social media security culture. In Information Security for South Africa (ISSA), p. 1-5, IEEE, August 2012.

[20] Talib, S., Clarke, N. L., & Furnell, S. M., Establishing a personalized information security culture. International Journal of Mobile Computing and Multimedia Communications (IJMCMC), 2011.

[21] Alnatheer, M., Chan, T., & Nelson, K., Understanding and measuring information security culture. PACIS 2012 Proceedings,p.144, 2012.

[22] Dzazali, S., & Zolait, A. H., Assessment of information security maturity: an exploration study of Malaysian public service organizations. Journal of Systems and Information Technology, 14(1), p. 23-57, 2012.

[23] Axelrod, Robert and Michael D. Cohen. Harnessing Complexity: Organizational Implications of a Scientific Frontier, The Free Press, 1999.

[24] David Wright and Paul De Hert (2014). Privacy Impact Assessment. Springer Science & Business Media, 2012

[25] Schein, E.H., Organizational Culture and Leadership (3rd Edn.). Jossey-Bass, 2004.

[26] Information Technology Security techniques Information security management systems Requirements. ISO/IEC 27001:2013.

[27] ISO/IEC 27001 Information Security Management: Securing your information assets Product Guide. Singapore: BSI Group Singapore.

[28] Mitchell, L.E., Corporate Irresponsibility: Americans Newest Export. New Haven: Yale University Press,(2001).