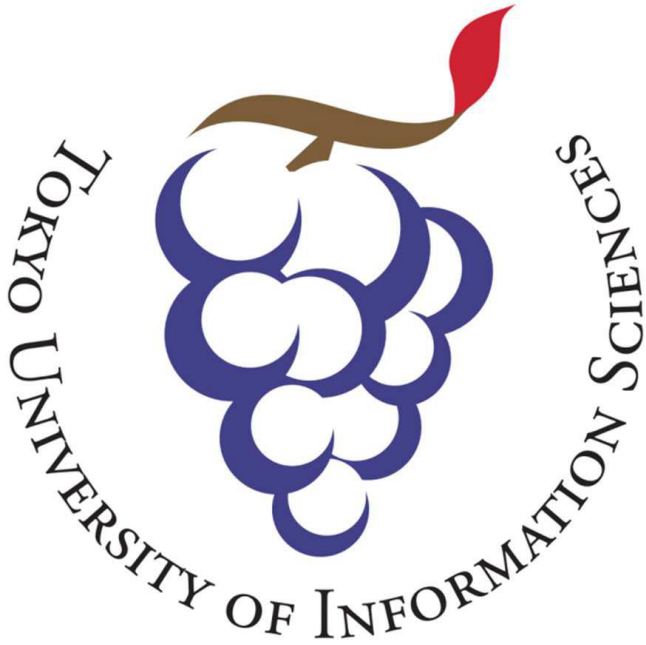
東京情報大学大学院総合情報学研究科
博士請求論文（平成２８年度）

タイトル　Identifying the Mechanisms of Information Security Incidents
情報セキュリティインシデントのメカニズムの明確化

指導教授　主査　　畠中 伸敏 教授
副査　　浅沼 市男 教授
副査　　櫻井 尚子 教授
副査　　綾野 克俊 教授

総合情報学専攻　環境情報系列
学籍番号 H14001
氏　　名 Abdullah Almubark

Identifying the Mechanisms of Information Security Incidents



A thesis submitted for the degree of Doctor of Information Science

by

Abdullah Almubark

Thesis advisor: Prof. Nobutoshi HATANAKA

Thesis co-advisor: Prof. Ichio Asanuma and Prof. Naoko Sakurai

Graduate School of Informatics

Tokyo University of Information Sciences

Japan

2017

フリガナ	アブドラ　アルムバラク
氏 名 （ 本 籍 ）	Abdullah Almubark　　（サウジアラビア）
学 籍 番 号	H14001
学位（専攻分野の名称）	博士　（総合情報学）
学 位 記 番 号	第 H10010 号
学位授与の日付	平成　29　年　3　月　25　日
学位授与の要件	学位規則第４条第１項該当
学 位 論 文 題 目	Identifying the Mechanisms of Information Security Incidents 情報セキュリティインシデントのメカニズムの明確化

論文審査委員	主査	畠中 伸敏 教授
	副査	浅沼 市男 教授
	副査	櫻井 尚子 教授
	副査	綾野 克俊 教授

論文内容の要旨

セキュリティ特性の時代的変化に対して，企業や機関は，柔軟に組織の体質を変化し，組織改善を図る必要があるが，セキュリティホールや脆弱性を放置し，外部からの攻撃を受けて，初めて，情報セキュリティ上に欠陥があることに気付く場合が多い．例えば，ソニー・コンピュータエンタテイメントのゲーム機 PSⅢのサービスサイトの１億人の個人情報の漏えいの事件の例では，open SSH 4.4 の古いバージョンのソフトを使用していたために，ハッカー集団からの侵入を容易にした．また，ハッカー集団による SQL インジェクションによる攻撃も行われ， Web 画面の脆弱性対策を怠っていた．このように，コンピュータシステムそのものに依存する脆弱性と，組織内部の人間に起因する組織上の欠陥を放置することは，経営者の責任である．

ところで，バーナードは，利益優先，効率重視，成果主義の結果として，組織要員の正当なる評価が歪められ，特定の人物による地位の独占を強められることを示した．また，賃金，名誉，威信が地位により，配分の差異があることを示した．これらが階層組織の逆

機能として働く結果，不祥事や事故が発生するとした．さらに，企業の生産活動の根幹となるテイラリズムでは，“能率”は，投入と産出の関係で決まるとしたが，サイモンは，組織の目標に企業活動の社会的価値が加えられてこそ，企業活動は意義あることで，組織目標と“社会的価値”の不協和により，社会的不祥事や事故が発生することを示した．

大日本印刷から個人情報 863 万件の漏えい事件，ベネッセコーポレーションの 2,300 万件の顧客データの漏えい事件は，いずれも，組織目標と社会的価値の不協和と，委託先の従業者により個人情報が漏えいする組織構造の中で発生している．これは，下請負契約者が，一次，二次から五次請まであり，最後は一人親方の構造となる建築土木業界と似た構造がある．この構造的欠陥が階層組織の逆機能となって，情報セキュリティインシデントの発生を助長している．

本研究の先行研究としては，一橋大学の星野崇宏教授を中心とするグループが，企業不祥事の組織要因として，43 の要因を挙げ，共分散構造分析を適用して，主要な組織要因を 11 項目に絞り込んだ．また，北海道大学の眞野脩教授は，“対等の立場において個々の人々や団体が，自己の個人的目的達成のために自主的に結んだ協定の結果生み出された組織（側生組織）”の存在を主張した．ベネッセコーポレーションの 2,300 万件の顧客データの漏えい事件は，委託先の従業者による個人情報の漏えいである．これは，眞野脩教授の主張した側生組織の負のメカニズムが出現した例である．

本研究では，星野崇宏教授のアプローチを，インシデント（事件）が発生した組織に適用し，主要な組織要因 11 個を同様に導き出した．

次に，主要な組織要因 11 個をもとに，2006 年から 2015 年までの過去約 10 年間に事件が発生した 186 企業に対して，Correspondence method を用いて，累積寄与率 56.8%で，組織帰属性，プロ意識，内部統制の軸を抽出した．この分析軸をもとに，得られた各企業のサンプルスコアに対して，階層型クラスタ分析を行い，事件が発生した企業の組織上の特徴を分類及び事件発生のメカニズムを明確にした．得られた企業グループは，自己自滅型組織，非帰属型組織，カモフラジュ型組織，無防備型組織，アウトロー型組織の 5 つである．

一方，ISO/IEC27001:2013(情報セキュリティマネジメントシステムの国際規格)の項番 5.3 には組織の役割，責任及び権限が規定され，同 6.1.1a)及び b)には，“意図した成果を達成できることを確実にする”，“望ましくない影響を防止又は低減する”とある．また，情報セキュリティの事件・事故の対策として，付属書 A には，114 の管理策と 35 の管理目的を掲げている．

本研究では，さらに，抽出した組織タイプで，それぞれ異なる組織要因により事件が発生していることから，個人情報保護マネジメントシステム、及び環境マネジメントシステムで適用されている局面と影響の関係を明確にする方法を、5 プロセスとして考案した．

事件が発生するアスペクト（欠陥のある組織活動）とインパクト（欠陥が情報セキュリティ上の事件に及ぼす影響）との関係を，それぞれに抽出した組織タイプごとに明確にし，それぞれの組織改善策を導き出し，日本のサウジアラビア大使館 IT 部門，及び，サウジアラビア大学イマム校アラビア語研究所で，5 プロセスの有効性を検証した。

Abstract

Security characteristics have changed, and as a result, companies need to changes their structures in order to promote flexibility and organizational improvement. In many cases, companies neglect security holes and vulnerabilities, realizing information security deficiencies only after they are attacked. For example, Sony Computer Entertainment leaked the personal information of 100 million people through its PS3 game console service site by using an old software version of Open SSH 4.4; which made it easy for hacker groups to invade the site. Because Sony failed to implement vulnerability countermeasures on its website, hacker groups were able to carry out an SQL injection attack. Clearly, it was the responsibility of Sony management to ensure that the organization properly addressed vulnerabilities directly derived from its computer systems; management also needed to concentrate on the organizational deficiencies caused by its people.

Barnard (1938) shows the result of a profit-first, efficiency-oriented and results-based has led to the corruption of the legitimate evaluation of the organizational members, and strongly enabling certain people to monopolize positions. Furthermore, differences in position caused several disparities in people's wages, reputations, and dignity. As a result of these acting as an inverse function of the hierarchical organization, scandals and accidents occurred. Furthermore, efficiency was determined by the relationship between investment and production in Taylorism, a doctrine that constitutes the basis of the production activities of companies. Simon (1997) shows that corporate activities are significant and meaningful only when their social value is adding to organizational objectives and that social scandals and accidents occurred due to disharmony between organizational objectives and social value.

In both cases of Dai Nippon Printing Co. leakage incidents of 8.63 million personal

information, and Benesse Corp. leakage incidents of 23 million customer data, the information security incidents occurred due to disharmony between organizational objectives and social values in an organizational structure, which allowed subcontractor's employees to steal personal information. This 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 and the bottom layer is comprised of self-employed craftsmen. This structural flaw constitutes an inverse function of hierarchical organization, which triggers information security incidents.

A previous study of this research in which 43 organizational factors of corporate scandals were conducted by a group led by Prof. Takahiro Hoshino (2008) of Hitotsubashi University. the number of organizational factors were narrowed down to the main 11 factors using a covariance structure analysis. In addition, Prof. Osamu Mano (1989) of Hokkaido University has insisted the existence of lateral organizations which are "a result of voluntary agreements between persons or groups of equal positions for the purpose of achieving their individual goals" (p.2). The incident at Benesse Corporation in which the data of 23 million customers was leaked by subcontractor's employees. This is an example of the negative mechanism of the lateral organizations that insisted by Prof. Osamu Mano.

In this research, applied Prof. Hoshino's approach to organizations in which incidents have occurred and similarly induced the 11 main organizational factors.

Based on the 11 main organizational factors, applied a correspondence method to 186 organizational samples in which incidents had occurred within approximately the last 10 years, between 2006 and 2015. With a cumulative proportion of 56.8%, three axes were derived and named as organizational attribution, professional consciousness and power of internal control. Based on the three derived axes, hierarchical cluster analysis was applied for the sample score

obtained for each organization. Then classified the organizational characteristics of companies with incidents and identified the mechanism behind the occurrence of the incidents. The result was five groups of bureaucratic self-destructive organizations, none-belonging organizations, purpose camouflage organizations, unguarded organizations and outlaw organizations.

On the other hand, the organizational roles, responsibilities and authorities are defined in Clause 5.3, and Clauses 6.1.1.a) and b) of ISO/IEC 27001:2013 stipulate “ensure the information security management system can achieve its intended outcome(s)” and “prevent, or reduce, undesired effects”. In addition, as measures of information security incidents, 114 management measures and 35 control objectives are listed in Annex A of ISO/IEC 27001:2013.

This research proposes a five-process method for identifying the relationship between aspects and impacts applied to PII (Personally Identifiable Information) protection management systems and environment management systems. This method is based on incidents resulting from different organizational factors specific to selected organization types.

For each type of organization, the research identified the relationship between the aspect (defective organizational activity) where the incident occurred and its impact (the effects of defects on information security incidents). Their respective organizational improvement measures then were induced. Finally, the effectiveness of the five-process method was verified, both for the IT department at the Saudi Arabian Embassy in Japan and the Arabic Institute at IMAM Branch of Saudi Arabian University.

Acknowledgement

I would like to express my sincere gratitude to my supervisor Prof. Nobutoshi HATANAKA for his continuous support of my PhD study and related research, for his patience, motivation, and immense knowledge. His guidance helped me throughout my research process and the writing of this thesis. I could not have imagined having a better supervisor and mentor for my PhD study.

Besides my supervisor, I would also like to convey my special thanks to Prof. Ichio ASANUMA and Prof. Naoko SAKURAI for my doctoral thesis review and supervision. Also, a special thanks to Dr. AYANO Katsutoshi from Tokai university, for his thesis review and his valuable comments. I am grateful for their kind acceptance to be reviewers and judges of my doctoral thesis as well as their helpful, constructive advice.

I also would like to thank Associate Prof. Osamu UCHIDA for providing support in statistical analysis. And Associate Prof. Yukiyo IKEDA for her unlimited support in organizational theory.

I am pleased to acknowledge all the students in Prof. HATANAKA's laboratory, particularly Yuhki NISHINO, for his continuous encouragement, support, and presentation discussions.

Last but not least, I would like to deeply thank and express special appreciation to my family, my mother, my wife, my daughter, and brothers and sisters who have always encouraged me with invaluable love. I would not have been able to complete and achieve this work without their encouragement and support.

Table of Contents

List of Figures

List of Tables

Introduction

It is often said that information security begins and ends with people, while information security incidents show no sign of significant decline, such as the Benesse Holdings, Inc. and JTB Corp leakage incidents. With the continuation of information security incidents, new information security technologies are being invented and applied in the workplace by organizations each year. However, it is impossible to eliminate information security incidents simply by applying additional security technologies. It is important to identify other factors that result in information security incidents within an organization. The part of information security technology constitutes only one of the factors that affect information security incidents. To provide a full consideration of the existing problems, it is necessary to study other aspects that derive from people and organizations.

This research aims to identify the organizational factors of information security incidents, and the structure of causes of organizational information security incidents. This research begins with summarizing Barnard (1938) discussion of the *functions of the executive* in relation to the inverse function of the hierarchical organizational structure. And summarizing Simon (1997) discussion of the *Administrative Behavior* concerning the sympathy between organizational objectives and social values. Followed by discussion of productivity proposed by Taylor (1911). In addition, the relationship between corporate culture and information security incidents is discussed, and the research identifies the causative factors behind information security incidents through several analyses. Finally, the research proposes how to improve upon corporate culture in order to remove organizational defects.

Chapter 1. Subject and background of information security incidents

1.1 Background of information security incidents

In today's world, information security incidents became global news (Laybats & Tredinnick, 2016, p.76), concerns about unauthorized access, cyber warfare, external threats, increased insider violation incidents, and corporate scandals have all brought increased attention to information security incidents (Whitman & Mattord, 2011, p.8). Information security incident is "a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security" (ISO/IEC 27001, p.2). According to Privacy Rights Clearinghouse (2010), the concern regarding information security incidents is still continuing to increase. In addition to the increase in information security incidents, an increase in the cost of incidents is appearing as well (Hobson, 2008), such as the direct cost "the direct expense outlay to accomplish a given activity" via lawsuits, reporting data breaches, or from indirect cost "the amount of time, effort and other organizational resources spent, but not as a direct cash outlay" such as lost revenue from reputational damage (Ponemon Institute, 2011, p.21).

Information security incidents are a challenge facing contemporary organizations operating within the context of the digital age. Many organizations protect their information assets by focusing on security breaches and extended expenses related to security technologies; however, it is impossible to eliminate information security incidents simply by applying additional security technologies. In the past, information technology's specific processes were utilized to target breaches of information, but these are no longer sufficient to provide for the demands of information security in the modern environment (Donahue, 2011).

It is important to identify other factors that result in information security incidents within an organization. Organizations that fail to address the key function of information security in the workplace often cite resource limitations as the reason behind their failure to implement sufficient security.

Security characteristics have changed over the last few years and the personalities of hackers, crackers, and attack methods have shifted. Hackers and crackers have become organized, and attack methods have also evolved from targeting individuals to attempting to expand their invasion into organizations. In order to cope with such changes, companies and institutions need to change their organizational structures to be more flexible and promote organizational improvement. In many cases, they neglect security holes and vulnerabilities and realize that there are deficiencies in their information security only after they are actually attacked. For example, in the case of Sony Computer Entertainment, the personal information of one hundred million people was leaked from its PS3 game console service site because an old software version of Open SSH 4.4 was used, which made it easy for hacker groups to break into it. Sony Computer Entertainment did not implement any vulnerability countermeasures on its website, which allowed the hacker groups to carry out an SQL injection attack. It is the responsibility of Sony management to ensure that the organization properly addresses vulnerabilities directly derived from computer systems and organizational deficiencies caused by its employees. The management's failures to fulfill its responsibilities were:

- Not performing a risk analysis and neglecting vulnerability flaws.
- Not performing a risk analysis and neglecting problems caused by people within the

organization.

Many organizations have ignored information security incidents in relation to organizational culture. Verton (2000) research suggests that, until the organizational culture is changed, information security will continue to face challenges similar to the ones seen today. In light of such theories, scholars have begun to examine organizational culture theory to understand how to reduce information security incidents (Vroom & Solms, 2004).

Organizational culture examines the behaviors within organizations. While many different definitions of culture exist, many focus on the collective behaviors and attitudes of the employees who make up an organization. Schein (2009) define culture as "culture is a pattern of shared tacit assumptions that was learned by a group as it solved its problems of external adaptation and internal integration, that has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems." (p.27). Research has established that these patterns of shared tacit assumptions are critical to the successful reduction of information security incidents; Nosworthy (2000) states that organizational culture "plays a major role in information security, as this may hinder change and determine what type of change is practical and what is not practical to be done based on the critical business processes." (p.340). Organizational culture is so crucial that it is the most important factor in the success or failure in an organization (Deal & Kennedy, 1982). Barnard (1938) found that inverse function reduced people's morale, and Simon (1997) shows that organizations increase their value and prevent the occurrence of corporate scandals only when their organizational objectives and social values are in harmony.

1.2 The subject of the research

This research tries to apply organizational theory to identify the organizational factors of information security incidents and identify the structure of the causes of information security incidents. In addition, an assessment and improvement process is proposed for corporate culture in order to remove organizational defects. The procedures of this research were as follows:

1. Inducing the main factor from organizational variables.

   Applying an approach which contains 43 organizational variables to information security incidents as same as organizational scandal to induce the main factors.

2. Inducing the analyzing axis in order to evaluate organizational incidents.

   Applying the main factors that have been induced from the 43 organizational variables to the collected 186 company samples of information security incidents and evaluating them by three axes after 186 company samples were scored concerning three axes.

3. Identifying the structure of the causes of organizational information security incidents.

4. Proposing assessment and improvement processes for corporate culture.

   Applying five processes to each group that has been classified to improve organizational defects.

5. Verifying the proposed assessment and improvement process of corporate culture to confirm the usefulness of the proposed assessment of corporate culture.

Chapter 2. The function of hierarchical organizations

The purpose of this chapter is to provide an understanding of the function of hierarchical organizations. This includes an introduction to the inverse function of the hierarchical organizational structure proposed by Barnard (1938) in his book *The functions of the executive*. In addition, an explanation of factors influencing the information security incidents within organizations such as individual, leadership and morals were provided. The chapter will be finalized by identifying the factors that present a set of candidate factors that influencing the information security incidents within organizations.

2.1 Introduction to the function of hierarchical organizations

The hierarchical organizational structure is a common structure within the context of modern business, with workers having varying levels of authority and power within the structure of the organization. Barnard (1938) studies the strengths and weaknesses of hierarchical organizational structures. He found that 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. The function of the top level of a hierarchical organization is significant given the high degree of influence and inspiration that is derived from it.

Barnard states that faults of structure "defective constitution" or "bad functioning, lack of solidarity or spirit, poor leadership or management" (p.6) present weaknesses, and the survival of an organization "depends upon the maintenance of an equilibrium of complex

character in a continuously fluctuating environment of physical, biological, and social materials, elements, and forces, which calls for re-adjustment of processes internal to the organization." (p.6).

Barnard notes that "formal organization is that kind of cooperation among men that is conscious, deliberate, purposeful," (p.4), Barnard also defines "formal organization" twice as "a system of consciously coordinated activities or forces of two or more persons." (p.73) and that "successful cooperation in or by formal organizations is the abnormal, not the normal, condition." (p.5). This indicates that individual characterizes the basic element in the organizational system. According to Barnard, an individual, is "a single, unique, independent, isolated, whole thing, embodying innumerable forces and materials past and present which are physical, biological, and social factors" (p.12); and the individual possesses certain properties: "activities or behavior arising from psychological factors to which are added the limited power of choice, which result in purpose." (p.13). In addition to that, individuals create the building blocks of every organization, regardless of which tier of power they perform in. Individuals' physical and biological limitations imply that "human organisms do not function except in conjunction with other human organisms" (p.11). This indicates that unique and independent humans cannot live alone, and each individual in a hierarchical organization is affected by his/her peers, those beneath him/her in the hierarchy, and those above him/her, creating a consistent flow of power, decisions, and functionalities.

While Barnard focuses his corpus of work on the physical components in an organization (i.e., the people), he also focuses on the morality of an organization and which morals are mandatory for a successful project. Person has the capacity of determination, and

power of choice. However, individuals are limited in terms of “biological faculties or capacities and the physical factors of the environment” (p.23). Barnard notes that “in fact, successful cooperation in or by formal organization is the abnormal, not the normal condition. What are observed from day to day are the successful survivors among innumerable failures” (p.5); this indicates that the difficulty in the task of achieving and securing cooperative systems. Within formal organizations, Barnard thought in real planning a process of developing and applying knowledge and intelligence to business problems, and thus, the idea that solutions to business challenges require the discussion of many, the perspectives of multiple arenas, and should be layered with the morality.

Barnard distinguishes between "effective" and "efficient" actions, “when a specific desired end is attained we shall say that the action is effective.”, “when the unsought consequences of the action are more important than the attainment of the desired end and are dissatisfactory, effective action, we shall say, is inefficient.”, and “when the unsought consequences are unimportant or trivial, the action is efficient.” (p.19). Organizational efficiency depends upon the contributions and inducements “that are specific and can be specifically offered to an individual” (p.142). Barnard notes that “efficiency of cooperation therefore depends upon what it secures and produces on the one hand and how it distributes its resources and how it changes motives on the other” (p.59). The specific inducements that may be offered are of several classes including “material inducements, personal non-material opportunities, desirable physical conditions, ideal benefactions, associational attractiveness, adaptation of condition to habitual methods and attitudes, the opportunities for enlarged participation, and the condition of communion” (p.142).

The function of the leadership of a hierarchical organization is significant; Barnard observes that “leadership is the indispensable fulminator of its forces.” (p.259) and considers leadership is the key factor in cooperation. Barnard states that “The inculcation of belief in the real existence of a common purpose is an essential executive function. It explains much educational and so-called morale work in political, industrial and religious organizations that is so often otherwise inexplicable” (p.87). This indicates that essential function of a leader is creating a sense of commitment and identification of followers. And leadership involves guiding others. Leaders must effectively convey meanings and intentions and receive them with sympathetic understanding. Leadership must get the job done and deciding on the right thing to do.

Barnard shows that in a cooperative system, the moral factor finds its concrete expression, underlining the necessity of leadership as “the power of individuals to inspire cooperative personal decision by creating faith: faith in common understanding, faith in the probability of success, faith in the ultimate satisfaction of personal motives, faith in the integrity of objective authority, faith in the superiority of common purpose as a personal aim of those who partake in it” (p.259). Another aspect of leadership is responsibility “it is the aspect of leadership we commonly imply in the word responsibility” (p.260), which is the “quality which gives dependability and determination to human conduct, and foresight and ideality to purpose” (p.260); thus, one part of leadership is to determine the quality of action which is the most important function of the executive.

Leadership and morals are being recognized for the significant function they play in terms of exerting an influence upon individual (employee) behavior. Focusing upon the

function of the organizational hierarchy is essential in framing the activities engaged in on behalf of individuals. It is through the top levels of the hierarchy that employees derive their guidance, and through the upper levels of the hierarchy that organizational objectives are upheld.

The initiatives implemented within organizations are directly affected by the top management and executive management of the organization. Such facts exhibit the important function played by organizational leaders in the context of information security and the support thereof. Top management in terms of information security provides the foundation through which policies are determined, communicated, and enforced. When organizations employ top-down pressure to maintain information security, employee behavior can be positively influenced. Given the noted function of the hierarchical organization in the maintenance of information security within organizations, following is a consideration of the inverse function of the hierarchical organizational structure thereof.

2.2 The inverse function of the hierarchical organizational structure

Barnard (1938) considers that the hierarchical organization's shortcomings include 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 weaknesses to the organization. The disparity between the level of compensation provided to organizational leaders and employees can lead to the development of lowered morale which may in turn lead to incidents and scandals. Such facts highlight the importance of establishing sufficient safeguards within

the context of organizations to preclude the engagement of the employees in illicit activities.

The hierarchical organizational structure is similar to that of the construction and civil engineering industry in which there are multiple layers of subcontractors, namely Tier 1 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 presents a lateral organization, which refers to "a group of two or more unit organizations may cooperate as a whole without a formal superior organization or leader" (p.110). Mano (1989) states that lateral organization is "created as a result of an autonomously agreement made by individuals and organizations in order to achieve their own personal purposes" (p.2). This indicates that lateral organization is composed of shareholders, creditors, consumers, raw material suppliers, and local governments, where subcontractors fall within the category of raw material suppliers.

2.3 The function of the status system

Barnard (1938) suggests that the following points ought to be considered as function of status systems and the hierarchical organization (the inverse Function).

Function of status system:

- The status system tends in time to distorted evaluation 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.

- It exaggerates administration to the detriment of leadership and morale.
- It exalts the symbolic function beyond the level of sustainment.
- Although it is indispensable for the cohesiveness and coordination of organizations, a hierarchy limits the resilience and adaptability of organizations.

The capacity of the hierarchical organization to negatively influence the behavior of employees in terms of morale is an additional weakness thereof. Employee behavior is largely affected by the morale that are in place within an organization. The morale of employees is comprised of colleagues, subordinates, and superiors. An example of how the hierarchical organization can have a weakness in terms of morale is that of Benesse Holding; when the morale of temporary staff appearing in the hierarchical structure had decreased, and complaints were filed for legitimate wages to be paid to a temporary staff member in spite of engaging in a significant operation in the business of Benesse Holding, This temporary staff member, using a USB, transferred the important personal information of the company externally without authorization and sold it to a name list provider.

2.4 Chapter summary

This chapter presented a comprehensive review of the function of hierarchical organizations and showed how such a bad functioning, lack of solidarity or spirit, poor leadership and morals shape the behavior of individual, controlled by the perception of

behavioral controls in place within the organization. Barnard considers that, the result of profit-first, efficiency-oriented and results-based has led to the corruption of the legitimate evaluation of the organizational members, and this strongly enables the monopoly of positions by specific people. Also, he considers that, shortcomings were disparities in the distribution of wages and honor and prestige among different positions; as a result of these acting as an inverse function of the hierarchical organization and scandals and accidents occurred. Benesse provides an example in which information security controls were not only lacking, but behaving outside the scope of acceptable parameters of behavior were even encouraged. The potential for the hierarchical organizations to create an environment in which the morals and leadership encourage noncompliance rather than discourage it presents a key weakness of the hierarchical organizational structure in terms of information security compliance and the establishment of organizational culture. In addition, the factors such as leadership, morals that could influencing information security incidents was examined in order to gain an understanding of the important factors that could substantially affect information security and corporate culture.

Chapter 3. Sympathizing with organizational objectives and social values

In the previous chapter, the function of the hierarchical organization that constituted the reason for organization scandals was discussed. This chapter provides how sympathizing between organizational objectives and social values prevent corporate scandals that is proposed by Simon (1997) in his book *Administrative Behavior*. This includes an introduction to Simon's suggestions for improving corporative objectives and corporate culture. Then investigate the 186-collected data to Simon's suggestions to see the similarity between scandals and incidents causes.

3.1 Sympathy between organizational objectives and social values

Simon (1997) defines communication as "any process whereby decisional premises are transmitted from one member of an organization to another. It is obvious that without communication there can be no organization," (p.227), this indicates the importance of efforts toward dialogue and mutual understanding (communication) among employees for organization. Simon expounds on the significance of efficiency with the expectation of elevating efficiency in order to accommodate the objectives of the organization, and he argues against the productivity of this concept, which is determined by the relationship between the inputs and outputs in Taylorism. Efficiency is normally determined in the relationship between investments and production. Simon states that "efficiency in the sense of a ratio between input and output, effort and results, expenditure and income, cost and the resulting pleasure, is a relatively recent term (p.276). By Taylor's definition, efficiency is the actual calculated ratio

compared to a standard work volume, and it becomes different from the simple input/output (investment/production) definition of efficiency. As something that is compared with the objectives and values of the organization, a different evaluation of efficiency as well as performance becomes possible. Operational efficiency will also generally demand maximum efficiency with limited resources. However, performance differs depending on the organization's objectives.

Simon 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. Consider the cases of JTB Corp. and Sony incidents, the information security incidents occurred due to disharmony between social values and organizational objectives in the organizational structure. At JTB, it was the responsibility of JTB management for keeping personal information on a machine that is reachable from the Internet. They should have considered isolating their networks. At Sony, the management also did not take any vulnerability countermeasures on its website, which allowed the hacker groups to carry out an SQL injection attack.

The organized society imposes its values and systems on the individual through the sympathize of organizational members and in the place of individual motives. The activities of the organization, in the scope of the consistency of societal and organizational values brought about by the sympathetic models they produce, are socially beneficial.

Sympathy is a significant for individual and organizations. By combining with organizational objectives and the social value, it is linked to the removal of organization incidents and scandals.

3.2 Organizational cause of incidents

The administrative principles of an organization were presents by Simon (1997) and relate to the challenges that organizations face when it trying to prevent scandals inside organization. By comprehensively considering the following items, it is conceivable that suggestions can be obtained for improving efficiency and preventing organizational incidents.

Administrative efficiency is increased by (p.48):

1. Specialization of the task among the 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).

Simon states that "Since these principles appear relatively simple and clear, it would seem that their application to concrete problems of administrative organization would be unambiguous, and that their validity would be easily submitted to empirical test. Such, however, seems not to be the case" (p.49).

Specialization, unity of command, span of control and organization's characteristic are explained as important causes for improving efficiency. However, consideration must be given to the adverse effects of these principles since they can cause organizational incidents. Nevertheless, these principles 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. Improvements that are realized in terms of administrative efficiency may nevertheless support the construction of a culture that is supportive of noncompliance.

The following are counterarguments to Simon's aforementioned ideas.

1. Specialization: The specialization of every field is called into question such as the location, function, etc.
2. Unity of command: Significant problems occur when the subordinate receiving orders holds more expertise than his or her superior. Even when a command is given priority, it will not necessarily elevate efficiency. Such issues are indicated also by Simon and other authors as irrationality in decision-making. As issues, it is called into question how and what is to be done, and whether they should be made commands.
3. Span of control: A control margin is not said to be good just because it is short. The dangers of the spread of bureaucracy are conceivable. Just because there are few hierarchical steps does not mean performance will improve. By narrowing the margin of control, the field of view of employees becomes narrow and there is the risk of losing sight of the truth. Significant problems, such as vertical division, bloating, and inefficiency, are now being brought forward, and the issue of narrow-mindedness is indicated.
4. Organization's characteristic: Organizations become problems by objectives, processes, customers, and locations. Here also, reciprocal contradictions are found. As the personality of management, such consistency is required.

3.3 Similarities between scandals and incidents

Data on 186 Japanese organizations where information security incidents took place from 2006 to 2015 were collected through reliable web sites in Japan such as “Security NEXT”, “DLP News”, and “Scan Net Security” archives as shown in Appendix B. These incidents were investigated using the items listed above in Section 3.2. It was seen that similar scandals and incidents had similar causes, as shown in Figure 1; they arose from social values or corporate culture. The scope of incidents and scandals is what differentiates them from one another, alongside the degree of involvement within the organization and its human resources throughout the hierarchy thereof.

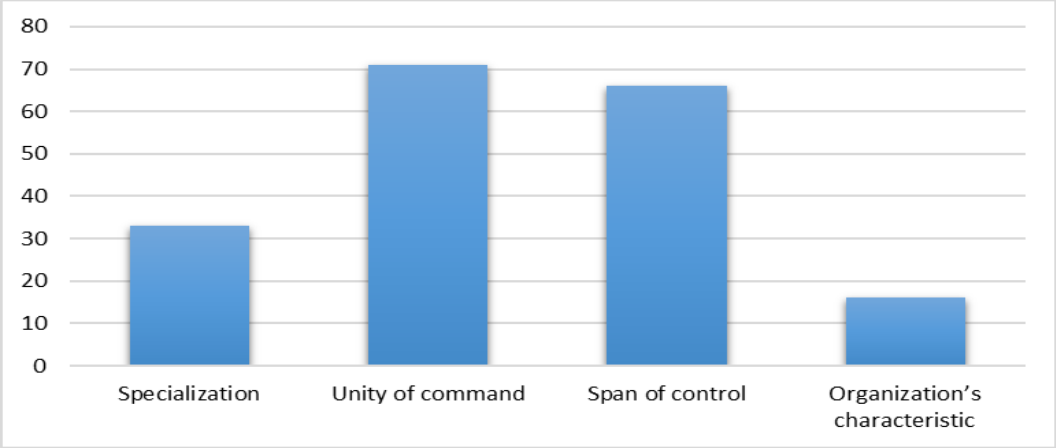


Figure 1. The 186-organizational sample of information security incidents that occurred from 2006 to 2015 were categorized using Simon’s (1997) four items explained above.

The structure of the organization and the degree of support for information security policies are markedly impactful upon the prevalence of information security incidents and scandals. The hierarchical organization entails both strengths and weaknesses in terms of supporting information security in the workplace context. The top management of the

organization and the position assumed in relation to information security and the enforcement thereof affects the perceptions of employees in relation to the information security policies. The intention of employees in turn affects their actual behavior, exhibiting the inherent link between the culture of the organization, the position of management in terms of information security, and the compliance behaviors of employees.

3.4 Chapter summary

In summary of this chapter, within the context of information security incidents, organization must sympathize organizational objectives and social value within the organization that are geared toward the elimination of organizational incidents and scandals. To that purpose, the loyalty of employees must be elevated with regard to organizational activities. The importance of employee compliance with information security is due largely to the key function of individual employees in terms of information security incidents. Internal organizational causes of information security incidents are common. Employees have access to confidential information, and through either intentional malicious activity or unintentional behavior that renders information security measures ineffective, may cause information security incidents.

Chapter 4. Productivity in Taylorism

The purpose of this chapter is to summarizing Taylor (1911) discussion of productivity in his book *The principles of scientific management*, and how employees can achieve information security. In addition, describing the four principles of scientific management proposed by Taylor.

4.1 Scientific management theory (Taylorism)

Taylor (p.12) proposes that productivity would increase by optimizing and simplifying jobs, and the directors of different managements should study a task in a scientific way. In addition, he advances the idea that employee and managers need to cooperate with one another. In order to substantiate his idea, he laid a model that can direct a task toward the scientific method in order to improve the efficiency.

The scientific management theory, also known as Taylorism, is one of the management theories that analyzes and sets the flow of work. Its primary objective is to improve efficiency, especially labor productivity. And despite the fact that scientific management as a distinguished theory or school of thought has become a thing of the past by the thirties of the twentieth century, the majority of its subjects still represent a part of management now. These topics include analysis, synthesis, logic, rationality, experimentation, work ethics, efficiency, the reduction of waste, the unification of best practice standards, and disregard for traditions that are maintained for the sake of tradition or only for the sake of protecting the social status of certain workers who possess a certain defined set of skills.

Taylor published in his book based on the following ideas (p.7):

1. The reduction in the level of productive efficiency in all businesses will result in huge losses.
2. The remedy of productivity deficiency rests in good management, for this is the fundamental guarantee in raising production rates.
3. Management is a science that depends on clearly defined set of rules, regulations, and principles, and reaching the targets necessitates the accurate implementation of these rules and regulations.
4. The rules, principles, and regulations of management can be applied on all the human activities and in all organizations regardless of their size, but on condition that these are applied in a proper and sound manner.

Taylor focuses in his researches and experiments on the discovery of methods that would increase the productivity of the worker and increase his wages on the basis of linking wages with production, by identifying the best way of working based on the study of "motion and time study" (p.25). To carry out the work after dividing it to partial operations. Taylor says that the function type of management should replace the military type in order for each function manager to have functional authority over all the workers.

Taylor (p.27) says that scientific management is more than being a research, planning and control method. It is an intellectual revolution or a new management philosophy that calls for a comprehensive change in thinking of management toward workers, and in the thinking of workers toward management towards one another.

Taylor based on the following views in drawing up his management philosophy (p.16):

1. The workers never tried to raise their productivity due to the nonexistence of a strong incentive that motivates them to increase their efforts.

2. The remuneration of an individual in an organization is set in accordance with his job and seniority and not in accordance with his capabilities, experience and productivity skills. This resulted in the decline of the performance level of the active worker to the performance level of a non-actives individual as long as he gets the same wages.

3. The ignorance of management in the amount of time required for completing a required job, which leads to losses in work and the rise in the cost of work.

4. The ignorance of members of management of systems to be followed to regulate the relationship between work and workers. And ways to be used to reduce manipulation and loss of time. Taylor observes the repetition of workers' evasion of work or pretending to be working without there being a real production. Taylor puts the blame for this phenomenon on two reasons:

    - Human Nature: The individual in his nature tends to laziness and the slow pace of work if there was no personal interest that secures for him an essential need.

    - The poor relationship of the individual with his colleagues or his managers leads to lower productivity.

5. The belief of some workers that the increase in their productivity would result in the dismissal of a number of them from work.

Taylor concludes from his study that there is a common interest beyond the limits between the employer and workers or between workers in the enterprise and the higher management, for the management asks the workers to achieve the highest level of it returns from work, and workers demand higher wages for their work. And Taylor believes that it is possible to satisfy both parties by giving the pay that corresponds with the size and type of work and, at the same time, it is possible to realize higher returns from work.

Taylor supports this view by saying that higher wages will give incentives to the workers to increase their productivity. And the cost per unit produced would be reduced. In fact, Taylor's thinking in this way was a revolution on the economic theories prevailing in that time to the effect that increasing yield cannot be possible except by reducing the cost of production, and the cost of production cannot be achieved except by the reduction of wages.

4.2 Taylor’s four principles of scientific management

Taylor developed four principles of scientific management (p.36). These principles are also known simply as “Taylorism”. Taylor's four principles are as follows:

1. Determining the type and amount of work required to be performed by each individual (which is what it is called today to determine specializations and responsibilities) based on scientific study and not on mere conjecture or random guess by the management.
2. The scientific selection of an individual who fits the position appointed for him, and providing him with a sufficient program of training until he increases his maximum efficiency.

3. The conviction of each of the board of management and workers of the justness of management organization and respecting its principles.

4. The division of duties and responsibilities where management specializes in the task of planning and leaves to the workers the task of implementation, and this is what Taylor calls the principle of separating planning from implementation.

It is clear that the Taylor's insistence on the use of scientific management, and streamlining the management process, the reduction of wasted time and of related unnecessary steps, is in fact an insistence on achieving the goals of the organization efficiently and also an insistence on the exhaustion of the employee's efforts, mind, and capabilities for the sake of the increase in productivity.

Thus, this scientific way that Taylor introduced in the management field had a certain negative aspect. For the insistence of organizations on adopting the principles of scientific management for the sake of achieving the objectives of the organization and increase of its annual production and profits, came at the expense of sacrifices on the part of the human element, where his movements are calculated, and he works in accordance with routine repeated steps that cause frustration and boredom and tedium. This led to the resistance of the worker to this method, for they seemed mere machines and that the primary goal of the scientific management is to increase production at their expense, so they opposed its implementation.

In fact, Taylor's interest to achieve adequacy of production and economy through the study of time and motion was a call to focus entirely on the project, and to attract attention to

the increase of productivity, to the extent that the study of management was limited to the study of guiding the administration of the organization, while it ignored the related social and human aspects of the workers.

4.3 Chapter summary

In summary of this chapter, from the foregoing that scientific management falls under the list of classical exemplary theories that describe what must be, and that it was based on one of the many aspects of an organization, that is, work, and it neglected the human being and human relations inside the organization which could lead information security incidents to the organization, and it did not care except about productive work on the level of the organization, and it did not give enough attention to the reality of interaction and exchange between the organization and the worker. In Taylorism, which is the basis of corporate production activities, it is said that efficiency is determined by the relationship between input and output. However, Simon considers that corporate activities are significant and meaningful only when their social value is added to organizational objectives and that social scandals and incidents occurred due to disharmony between organizational objective and social value.

Chapter 5. Relationship between corporate culture and information security incidents

Information security incidents is critical for organizations to survive, and there is still an increasing interest to study information security incidents from corporate culture perspective. Therefore, this chapter is seeking to explore the relationship between corporate culture and information security incidents. And focuses on the effect of strong corporate cultures and organizational commitment as important aspects for enhancing information security.

5.1 Organizational culture and misconduct

Hofstede (2010) 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 (p.5). Individuals living and operating within the same social environment tend to share these elements. Veiga (2015) states that “the internal influences on compliance is the organizational culture” (p.23). Corporate culture and information security incidents are intrinsically linked to one another, and the concepts are researched simultaneously (Shover & Hochstetler, 2002). Thus, within organizations, culture influences the perspective applied to organizational facets, including information security.

Shover and Hochstetler (2002) found that the 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.

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 (Schein, 2009, p.78). Culture is influential upon the behavior of employees at large given its expansive impact upon the stakeholders therein.

Hoshino et al. (2008) examined the function 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 (p.170). 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 (Niekerk & Solms, 2010).

Veiga and Eloff (2010) asserted that an organization's approach to information security must focus on employee behavior. Gebrasilase and Lessa (2011) stated that information

security culture comprises a set of characteristics that are valued by the entirety of the organization. This emphasizes the importance of culture within an organization.

Alfawaz et al. (2010) noted the difficulty in understanding the complex dynamics and uncertain characteristics related to an organization's 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 the organization. Culture may potentially be quantified through a consideration of social-cultural factors within an organization (Kruger et al., 2010).

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 essential to establishing and reinforcing the protection of information assets; the most important is human cooperative behavior (Niekerk & Solms, 2010). Therefore, 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 (Veiga & Eloff, 2010).

Niekerk & Solms (2010) researched information asset security and found employees to be the greatest threat to information security, often due to negligence, intentional action, or 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 are minimized and managed; however, the accomplishment of this goal is not simple (Alfawaz et al., 2010).

Within the modern business environment, industry experts are increasingly demanding a stronger focus on information security. Information security must be incorporated into

organizational strategies in order to be effectively addressed; however, despite its importance, there is no clear blueprint through which a firm may achieve a strong organizational culture (Kayworth & Whitten, 2010). The values associated with organizational culture are manifested in the practices and activities within the organization in relation to information security management (Alfawaz et al., 2010).

Focusing on information security within organizations is a comprehensive process. Kayworth and Whitten (2010) conducted qualitative research which involved interviewing 21 information security executives from 11 organizations, and found that information security strategies are complex. Generally, this involves a strategically-focused information approach that incorporates not only IT products and solutions but also social alignment and organizational integration mechanisms. These strategies are often managed through the institution of a control-based compliance model (Hedström et al., 2011).

5.2 Information security in the workplace

The mitigation of information security threats depends on determining the source of the threats. Malicious threats come from both within and without the organization. Often, such threats stem from organizational insiders. Insiders are capable of causing greater damage due to their position; thus, they must be quickly identified and subsequently targeted using countermeasures. Information security countermeasure strategies are a means of addressing particular threats (Coles-Kemp & Theoharidou, 2010). Given the high level of threat that may emerge from organizational insiders, it is important that measures are implemented to govern the behavior of employees, while also precluding the realization of unnecessary risk, such as

the barring of the use of personal USB devices or the surfing of non-work websites on company hardware.

Information security strategies must be as complex as the threats that face modern organizations. The socio-technical approach is a means to achieve three objectives. The first of these is achieving a balance between security essentials and the need to enable the business. Security measures cannot be cumbersome to the point that they negatively impact productivity, however must be sufficiently comprehensive to protect against all potential threats. The next objective of the socio-cultural approach to information security is the maintenance of compliance. Adhering to regulatory standards is essential to ensure the legitimacy of the organization's operations. The final objective of the socio-technical approach to information security is to ensure that the strategy is appropriate for the organizational culture (Kayworth & Whitten, 2010). The fit of the strategy employed is influential upon its capacity to function effectively.

Employees are central to the protection of organizational information, by embedding security into the corporate culture, employee behaviors that protect the information of the organization can be "positively influence employee behavior." (Lim et al., 2010, p.463).

Employee compliance is one of the more difficult facets of information security measures, which highlights the importance of enforcement, including monitoring. One way to directly control and observe employee behavior in relation to information security is by monitoring employee computers (Greene & D'Arcy, 2010).

The workplace itself and the culture in place therein plays a key role in the support of information security. According to Vacca (2013) "Corporate culture can drive whether

monitoring of any kind is even allowed" (p.182). Within the context of the workplace, employees are provided with means through which data, oftentimes sensitive or confidential, is transmitted. The measures in place within the organization determine the ingress and egress of data, with the employees executing such measures (Vacca, 2013). The function that is allocated to information security affects the level of prioritization that it is afforded within both employees and management alike.

Research conducted by Hu et al. (2012) found that the position of top management towards security in turn markedly influences the security compliance behavior engaged in on behalf of employees. The researchers employed survey data in addition to structural equation modeling in order to explore hypotheses concerning the relationships between top management and employees' security compliance behaviors. The study found that "top management participation in information security initiatives has significant direct and indirect influences on employees' attitudes towards, subjective norm of, and perceived behavioral control over compliance with information security policies" (Hu et al., 2012, p.615). Employee adherence to security policies is driven by the position of top executives, exhibiting the importance of clarifying and quantifying information security in the workplace context.

It is not only the function of management that is central to the realization of the security-related objectives of the organization, but also the employees. Hu (2012) found that the relationship between top management's participation in information security measures and employee compliance with information security is "mitigated by the employees' cognitive beliefs about compliance with the information security" (p.615). To optimize the compliance of employees with the information security of the organization, it is thereby important for top

management to undertake a proactive function in the shaping of employees' compliance behavior.

The compliance undertaken on behalf of employees is regulated by their perception of information security compliance and the importance thereof. Thus, the attitudes and beliefs of employees related to information security in turn affects the degree to which they incorporate information security concerns into their work. Management has the capacity to proactively shape the perception of employees concerning information security. Managerial support and shaping in terms of employee information security compliance can be used to reinforce deterrent-oriented remedies to information security related issues (Hu et al., 2012). Management can improve upon the perception of employees related to information security compliance, thereby complementing other supporting frameworks in place to ensure information security adherence throughout the organization.

One aspect of information security that is often overlooked by organizations is the determination of the monetary cost, or value, of information security. Employees who are subjected to rigid information security policies and procedures without first being made to thoroughly understand the reasoning behind such practices may view them as a liability or inconvenience more so than an essential element of their workplace behavior. Information security breaches have very real monetary implications, and can cost organizations sizeable sums of money. Facilitating the understanding of employees in terms of how information breaches affect their ability to receive raises further establishes the link between employee behavior and information security.

To measure employee behavior related to information security, Padayachee (2012)

studied the “extrinsic and intrinsic motivations that influence the propensity toward compliant information security behavior” (p.1). Employee behavior in this regard comprises a set of core information security activities that must be adhered to by end-users to promote security.

Information security within an organization is also affected by social media. Social media provides both an opportunity and risk for organizations, underlining the importance of effectively managing all facets of electronic information within an organization (Oehri & Teufel, 2012). Talib et al. (2011) found that information security within an organization must be complemented by further research into how technology is used by employees. By focusing on overall information security behavior, an all-around information security culture may be established that is present within both the home and office environment (Talib et al., 2011).

Alnatheer et al. (2012) endeavored to develop a measurement for information security culture. The purpose of the research was in recognition of the apparent lack of a clear conceptualization of information security culture, and the factors that constitute and influence it. 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 ownership” (p.3) within an organization. Dzazali & Zolait (2012) 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 the technical factors are fewer. This indicates the importance of individual perception and risk management efforts.

Information security is largely influenced by organizational culture, as clearly seen through the literature reviewed above.

Chapter 6. Inducing the main factors from organizational variables

6.1 Factors concerning information security incidents

The factors and issues related to organizational scandals were proposed by Hoshino et al. (2008), a research group at Hitotsubashi University; Hoshino et al. states that “the culture of fraud and neglect of violations at workplace is effected by organizational cultures involving trust in the workplace, sectarian behavior, belonging scale and by management-operative cultures that consist of leadership, development of compliance, employment continuity or security, rules of employment, segregation of duties, result-based and that trust in the workplace” (p.160), sectarian behavior, belonging scale are also influenced by leadership, development of compliance, employment continuity, rules of employment, segregation of duties, result-based, as shown in Figure 2 that modified from Hoshino, et.al (2008, p.161, Figure 1).

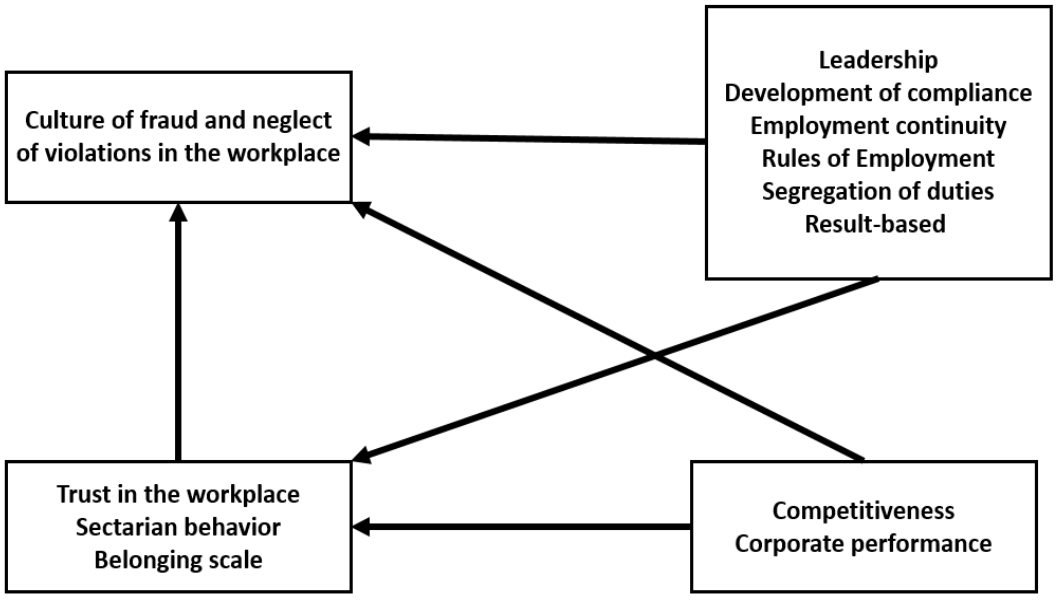


Figure 2. Relation between variables- modified from Hoshino, et.al (2008, p.161, Figure 1)

Hoshino et al. noted that “Compliance as a word does not only define the system construction by the management acts, but sometimes includes the positive observance of laws and morals” (p.162). However, the system which is constructed by the management acts must be divided to discuss from the observant culture. Therefore, the side of the compliance system is named as “the development of the compliance system.” (p.162). The hypotheses for the organizational culture and the management-operative variables are as follows (Hoshino et al., 2008, p.162-164):

(1) The “culture of fraud and neglect of violations in the workplace” is weak in organizations with higher “moral leadership”.

(2) The more eager the effort to “the development of compliance system” is, the more it degrades.

(3) The culture of fraud and neglect of violations in the workplace deteriorates when “the employment is secured” but the contrary feasibility often occurs.

(4) The culture of fraud and neglect of violations in the workplace is controlled when “the work rules” are austere.

(5) The culture of fraud and neglect of violations in the workplace is controlled when “the segregation of the duties” enacted.

(6) The culture of fraud and neglect of violations in the workplace is augmented when “the resultism” is stronger.

(7) The culture of fraud and neglect of violations in the workplace is augmented by “competitiveness,”.

(8) The culture of fraud and neglect of violations in the workplace is lowered when “the

corporate performance" is satisfactory.

(9) The culture of fraud and neglect of violations at workplace is lowered when "the trust in the workplace" is high.

(10) The culture of fraud and neglect of violations in the workplace is reinforced by "sectarian behavior".

(11) The culture of fraud and neglect of violations in the workplace is augmented by "the belonging scale."

It is natural to expect that the fraud and neglect of violations in the workplace becomes hard carry out when the manager demonstrates his or her moral leadership. As same as the efforts to the development of the compliance system.

Highly secured employment is considered to produce the organization faithfulness and loyalty and prevent from illegal acts that cause the organization's reputation to crumble. However, in some organizations, highly secured employment produces factions and might cause the outbreak of incidents.

In addition, at workplaces strictly applied the work rules, the culture of neglect of injustice and violations ought to be controlled. The segregation of the duties is considered to explain the strength of the superficial organization structure, and when the degree of freedom of the discretion at work is low, the space to conduct frauds is considered to be small. In organization with the high resultism, it is apprehended to conduct frauds in order to give personal results, and to be involved in the sequestration of frauds in order to achieve high evaluation.

Variables that are not always directly operative by management, but are expected to influence scandals' occurrence, competitiveness and corporate performance are introduced. The neglect of injustice and violations is augmented by competitiveness, and lowered when corporate performance is satisfactory.

The hypothesis of these organizational cultures is the culture of fraud and neglect of violations at workplace is lowered when the trust at workplace is high, reinforced by the sectarian behavior, and augmented by the belonging scale.

In this research, the hypothesis of Hoshino et al. (2008) was used to explain the defects of organizational culture and information incidents. And induce the main factors that concern information security incidents.

6.2 Questionnaire and data collection

In this research, a questionnaire survey that was used by Hoshino, et.al (2008, p.163, Table 1.) is adopted as an essential tool for data collection. 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 organizational variables were classified into 8 sections as shown in Appendix A.

The observed organizational variables concerned with the section "culture of fraud and

neglect of violation in the workplace" (Hoshino, et.al, 2008, p.163, Table 1) 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 was used for covariance structure analysis.

After the data were collected, the returned responses were organized, and the data were uploaded into the Statistical Package for Social Sciences (SPSS) program version 22. As shown in Table 1, the returned participants responses indicated that 37% of participant's age from 31 to 40 was the majority, as well as participant's gender "male" was the highest employee at 81%. In addition, three questions were distributed to participants in order to discriminant between groups regarding being violated by a virus (Yes, No). The questions and responses were as follows:

1. I have been violated by a virus to my computer (78%)
2. I have looked into the password of another person (36%)
3. I have shared my password with another person (14%)

Table 1. Returned participants' response

Participants' Answers		92%
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

6.3 Induce the main factors

After obtaining data concerning the 43 organizational variables, it is important to verify the validity and reliability. Validity refers to the extent to which what is intended to be measured is actually being measured. Reliability indicates whether an instrument measures something consistently. Kline (2011) refers internal consistency reliability as “the degree to which responses are consistent across the items within a measure. If internal consistency is low, then the content of the items may be so heterogeneous that the total score is not the best possible unit of analysis for the measure.” (p.69).

Cronbach’s alpha coefficient is the most common measurement for internal consistency, which calculates the estimated correlation of a set of items and true scores. A low Cronbach’s alpha coefficient indicates that variables may be so heterogeneous that they perform poorly in representing a measure. Pallant (2005) states that “one of the most commonly used indicators of internal consistency is Cronbach’s alpha coefficient. Ideally, the Cronbach alpha coefficient of a scale should be above 0.7” (p.90). Cronbach’s alpha above 0.70 is considered an acceptable indicator of internal consistency and values of 0.60 to 0.70 are at the lower limit of acceptability. Table 2 presents the Cronbach’s alpha. In addition, it has been suggested that analyses of the item-total correlations for the items should be considered. Pallant notes that “The other information of interest is the column marked corrected item-total correlation. These figures give you an indication of the degree to which each item correlates with the total score. Low values (less than 0.3) here indicate that the item is measuring something different from the scale as a whole.” (p.92).

Lu et al., (2007) refers item-total correlation as “a correlation of an item or indicator

with the composite score of all the items forming the same set." (p.855). If all variables share a common core of the same construct, the score of each variable, and that of the entire construct, should be highly correlated (Koufteros, 1999). It is recommended to perform the purify the measure (Churchill, 1979, p.68) by eliminating measurement error before determining the factors that represent the construct.

Table 2. Cronbach's alpha coefficient and proportion rate

	Number of Items	Proportion Rate	Cronbach's Alpha Coefficient
Culture of fraud and neglect of violation	8	0.623	0.813
Trust in the workplace	5	0.697	0.891
Sectarian behavior	9	0.636	0.921
Belonging scale	5	0.659	0.870
Moral leadership	3	0.758	0.837
Leadership in the workplace level	4	0.788	0.710
Development of compliance system	3	0.799	0.874
Other single indicators	6	0.607	0.868

The values of the alpha coefficients for all the construct scales ranged from 0.710 to 0.921, suggesting good internal consistency and reliability for the scales with this sample. And the value of the item-total correlation is corrected through using SPSS. The corrected item-total correlation excludes the score of a variable of interest when calculating the composite score. And the results of item-total correlations presented in Tables 3 to 10, and show that all corrected item-total correlations were greater than 0.3.

Table 3. The item-total correlations of culture of fraud and neglect of violation

Variables: Description	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
Did you ever disobey the basic rules in your workplace?	.387	.834
Have you ever made false reports in your workplace?	.653	.774
Have you seen the performance of dishonest means with respect to important decisions in the past?	.693	.773
In your workplace, did your manager ever neglect the fraud even knowing them?	.627	.777
In your workplace, did your manager ever instruct you to conceal the fraud?	.630	.780
Do you have an atmosphere that earns a profit, even by illegal act?	.635	.779
For problems, such as illegal act happened in other organizations, do you have an atmosphere that your organization would not take the same actions?	.544	.793
Does an illegal act done by the group of decision making in your workplace?	.429	.820

Table 4. The item-total correlations of trust in the workplace

Variables: Description	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
Do you think the coworker can collaborate closely in your workplace?	.749	.864
Do you think the information transfer between members is performed widely and smoothly in your workplace?	.693	.877
Do you think your co-worker reliable at work?	.738	.866
Do you think your manager reliable on work?	.732	.867
If you put priority on doing the right thing, will your manager and co-worker support you?	.761	.862

Table 5. The item-total correlations of sectarian behavior

Variables: Description	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
Do some people form a strong conspiracy in your workplace?	.733	.911
In your workplace meeting, do some people work together to get a favorable resolution with complicity?	.822	.905
Is it difficult for you to propose an opposite opinion against the members of mainstream faction in your workplace meeting?	.581	.923
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?	.776	.908
Are there any "escape goat" (people to sacrifice) in your workplace, so that anything inconvenient can be attributed to them?	.795	.907
Are the people surrounded by the yes-man subordinate leaders of your organization or workplace?	.818	.906
Does the subordinate who does not do the present (gift) for the manager become disadvantageous by promotion in your workplace?	.853	.904
Are the individual who actively speak sound arguments labeled as "problem child", and ignored or shunned in the workplace?	.758	.910
Are the claims of some of members almost all accepted regardless of its content?	.391	.932

Table 6. The item-total correlations of belonging scale

Variables: Description	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
In a face-to-face meeting with the opponent, it happened that you could not express your dissenting opinion.	.607	.864
In a meeting, even the same proposal will have different result in being passed or not depending on the proponent.	.740	.832
When trouble occurs, the atmosphere there is more of "whose responsibility it is" than of "what the cause is".	.728	.835
People are evaluated more from likes and dislikes than the way they do work.	.714	.838
The priority of work is often decided by who has requested.	.690	.844

Table 7. The item-total correlations of moral leadership

Variables: Description	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
In your workplace, does a manager emphasize restraint of the injustice definitely?	.584	.884
Are the managers in your workplace behaving as the moral model for others?	.766	.709
Have the managers in your workplace a strong sense of mission?	.759	.715

Table 8. The item-total correlations of leadership in the workplace level

Variables: Description	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
Does the top of your workplace put entrenchment in the first place instead of self-sacrifice?	.433	.683
When you are confused in a judgment, will your manager give appropriate Legal instructions for the entire workplace?	.521	.632
Does your manager brandish their power to the subordinate one hand, but behave obediently to people in the upper position?	.445	.677
Have your manager shown enough leadership on work?	.594	.588

Table 9. The item-total correlations of development of compliance system

Variables: Description	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
Does a system to check the manager function effectively in your organization?	.689	.883
Does enough information disclose it at the time of decision making in your workplace?	.791	.792
Do you aim to establish a compliance (legal and ethical compliance) in your workplace?	.799	.786

Table 10. The item-total correlations of other single indicators

Variables: Description	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
Is the regular employee in your workplace alienated except for special conditions?	.631	.853
Have your employment regulations been strictly followed in workplace?	.683	.843
Has the work objective of each person been clear every day?	.775	.826
Do you let you reflect achievements and the result that each person achieved when decision of the annual raise in salary, promotion in the last year directly in your organization?	.769	.827
Is there fierce competition existing in the market activities in your company (organization)?	.563	.862
Does your organization produced a good performance and been highly evaluated during the past decade?	.585	.859

Exploratory factor analysis (EFA) was applied to analyze the correlations of a large number of variables to define the underlying structure by identifying factors (Hair et al., 2010). An exploratory factor analysis is “a useful scale development technique for reducing a large number of indicators to a more manageable set. it is particularly useful as a preliminary analysis in the absence of sufficiently detailed theory about the relations of the indicators to the underlying constructs (Gerbing & Anderson, 1988, p.189).

Factors were extracted from the variables. All coefficient alpha values were higher than 0.7, which indicates that all 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 (0.623 Proportion ratio), the coefficient alpha for the total number of points was high at 0.813, 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 (0.697 Proportion ratio), the coefficient alpha was high at 0.891, and it was found that the items can be used as a scale with one dimensional properties.

3. Sectarian behavior

   After developing nine question items that conceivably measure sectarian behaviors, a single factor was extracted, the proportion ratio was high at 0.636, and the coefficient alpha was high at 0.905.

4. Belonging scale

   Five items were used in this analysis. A single factor was extracted, the proportion ratio was 0.659, and the coefficient alpha was high at 0.870.

5. Moral leadership

   Three question items here that are conceivably related to corruption and the neglect of violations were used to make measurements. The proportion ratio was 0.758, and the coefficient alpha was at 0.837.

6. Leadership in the workplace level

   After measuring the moral leadership of management and managers at the workplace level using four question items, the proportion ratio was 0.788, and the coefficient alpha was high as three items at 0.710.

7. Development of a compliance system

   Three question items were given to measure whether such organizations were aiming toward compliance management or carrying out information disclosures. The proportion ratio was 0.799, and the coefficient alpha was 0.874.

8. Other single-item indicators

   Items that were conceivably sufficient in obtaining 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" (Hoshino, et.al, 2008, p.163, Table 1.) The proportion ratio was 0.607, and the coefficient alpha was 0.868.

Through the results of the exploratory factor analysis, variables concerned with information security incidents have been induced. The results are shown in Table 11. The results indicate that all eleven factors are valid for confirmatory factor analysis.

Table 11. Results of induced variables

		Factor										
		1	2	3	4	5	6	7	8	9	10	11
1	Q20	0.948										
	Q18	0.887										
	Q17	0.869										
	Q19	0.829										
2	Q26		0.831									
	Q25		0.827									
	Q24		0.799									
	Q27		0.728									
3	Q9			0.898								
	Q11			0.818								
	Q12			0.764								
	Q10			0.734								
4	Q41				0.877							
	Q40				0.771							
	Q39				0.606							
5	Q36					0.839						
	Q37					0.703						
	Q35					0.698						
6	Q29						0.790					
	Q30						0.765					
	Q28						0.339					
7	Q3							0.712				
	Q2							0.652				
	Q6							0.612				
8	Q5								0.818			
	Q4								0.505			
9	Q8									0.700		
	Q7									0.682		
10	Q33										0.771	
	Q31										0.401	
11	Q34											0.564
	Q32											0.476
Coefficient Alpha		0.913	0.859	0.884	0.819	0.853	0.784	0.713	0.601	0.703	0.662	0.686

6.4 The analysis results

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. In addition, it has been shown that culture of fraud and neglect of violations decreases in organizations that score higher in the development of compliance systems. Its influence, however, is limited.

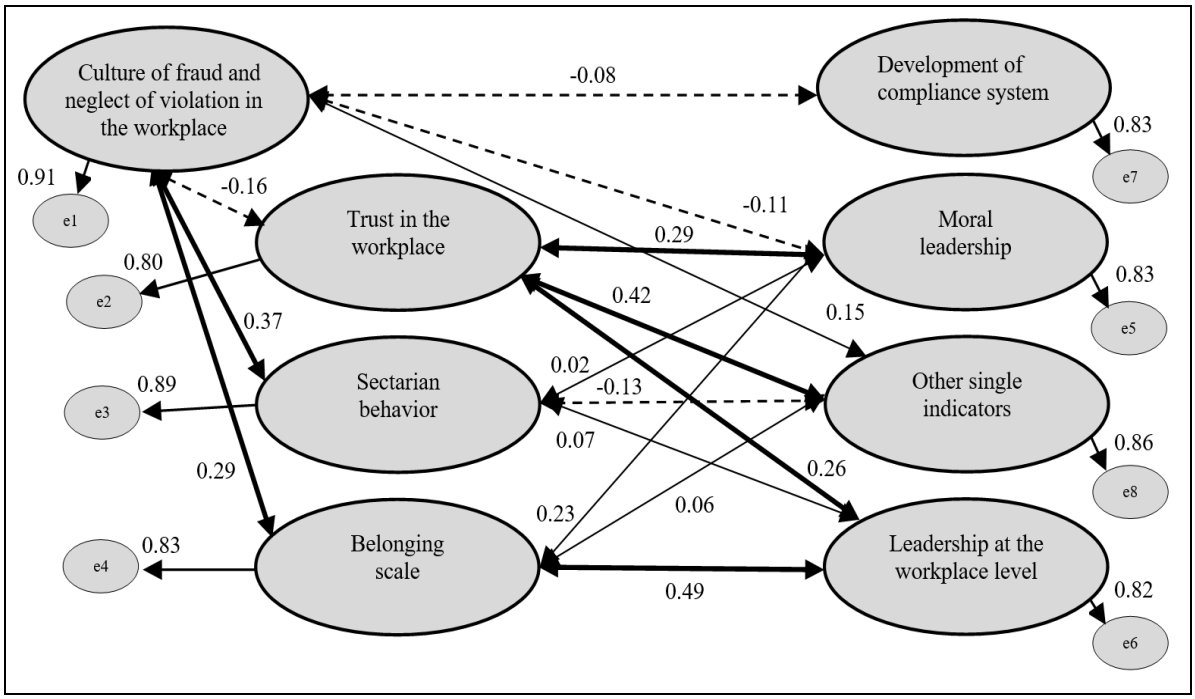


Figure 3. Result of confirmatory factor analysis (AGFI= 0.848, CFI= 0.929, RMSEA = 0.055)

Table 12. Estimates of correlations among exogenous variables

	Sectarian behavior	Belonging scale	Trust	Other indicator	Compliance	Moral	Culture of fraud	Leadership
Sectarian behavior	1.000	0.497	-0.239	-0.132	-0.029	0.019	0.372	0.071
Belonging scale	0.497	1.000	-0.089	0.068	0.103	0.235	0.291	0.306
Trust	-0.239	-0.089	1.000	0.417	0.428	0.296	-0.161	0.263
Other indicator	-0.132	0.068	0.417	1.000	0.71	0.492	0.153	0.597
Compliance	-0.029	0.103	0.428	0.71	1.000	0.617	-0.086	0.298
Moral	0.019	0.235	0.296	0.492	0.617	1.000	-0.113	0.404
Culture of fraud	0.372	0.291	-0.161	0.153	-0.086	-0.113	1.000	-0.051
Leadership	0.071	0.306	0.263	0.597	0.298	0.404	-0.051	1.000

At the same time, whereas moral leadership is effective on the suppression of a culture of fraud and neglect of violation in the workplace, leadership in 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, only has limited effects on a culture of fraud and neglect of violation in the workplace. In addition, it was shown that moral leadership by the management and trusting relationships in the workplace are more important than the development of compliance systems. This indicates that, to prevent information security incidents at the level of the workplace in the future, it is important to improve the organizational culture that include trust, sectarian behavior, belonging scale, and moral at the level of the workplace and organizational members. The willingness of organizational members to engage in information security behaviors is determined by the position of management related to information

security allegiance and enforcement, and the perceived behavioral controls that are in place. Through strong organizational culture to enforce information security compliance among organizational members, individual subjective factors that may influence noncompliance are mitigated, thereby supporting the overall information security in workplace. In addition, it should be maintaining the social trust of an organization to preventing information security incidents.

Chapter 7. Inducing the analyzing axis in order to evaluate organizational incidents

7.1 Gathering the 186 organizational samples (company) which have incidents.

To induce the analyzing axis, it was necessary to gathered organizational sample. Accordingly, data on 186 Japanese organizations in which information security incidents took place from 2006 to 2015 were collected through reliable web sites in Japan such as “Security NEXT”, “DLP News”, and “Scan Net Security” archives as shown in Appendix B.

7.2 Correspondence between the company incidents and the main factors

Eleven factors regarding information security incidents have been induced in chapter 6, using these eleven main factors for corporate culture. The collected 186 organizational samples of information security incidents were evaluated using the following corporate culture variables; “1” was assigned if there was a correspondence, and “0” was assigned in other cases.

Variables for corporate culture:

1. Deterioration of values: There is no information security education, or security awareness is low.
2. Freewheeling corporate culture: Security rules are not followed, or hidden manuals exist.
3. Hands-off policy: Managers’ intentions are not clear.
4. Unclear objective of the management: Lack of consistency in management, such as precarious day-to-day management.

5. Not customer-oriented: Communication with customers after information security incidents is not appropriate.
6. Unmanaged organization: There are no internal controls in the organization.
7. Lack of a sense of belonging: Information security incidents are caused by subcontractors' employees and contractors (copartners).
8. Organization with numerous dissatisfactions: Whistle-blowing.
9. Organization with no autonomous control: Information security incidents are detected only by indications from outside of the organization.
10. Organization without corrections: Multiple occurrences of information incidents.
11. Organization without leadership: Leaders are frequently replaced.

7.3 Applying the correspondence method to the 186 organizational samples

The research procedure to identify incidents using statistical analysis involved the following:

- Correspondence analysis was used as the method of deriving factors.
- Hierarchal cluster analysis was used as the grouping method, the Centroid method for Unification criteria, and Degree of similarity for the Euclidean distance between sample scores.

In assessing the corporate culture, security measures and previous information incidents were investigated to ensure an objective evaluation.

The corporate culture evaluation data were analyzed using the correspondence analysis

to identify factors that affect information security incidents. The organizational variable of corporate culture for past information security incidents was induced. Through these analyses, the relationship between the pattern of information security incidents and the factors of corporate culture was derived. As the cumulative proportion rate of the third factor was found to be 0.568, which is almost 60%, the following three factors were derived and named as:

1. The first factor indicates the highest value (1.314) in “Uncorrected organization”, and it was inferred to be caused when more than one information incident occurred, namely, multiple occurrences of information incidents. And it shows the attribution of social status and organization. For these reasons, it was suggested that the first factor named as “Organizational Attribution”. Taking into account Figure 4 and Table 13, the variables that were positive including “Uncorrected organization, Freewheeling spiritual features, Organization without leadership, Dissatisfied organization, Unclear objective of the management, and No customer-orientation” were considered to be more “liberal profession”. On the contrary, the lowest values including “Deterioration of values, Hands-off policy, Organization with no autonomous action, Unmanaged organization, and Lack of a sense of belonging” were inferred to be “belonging organization”.

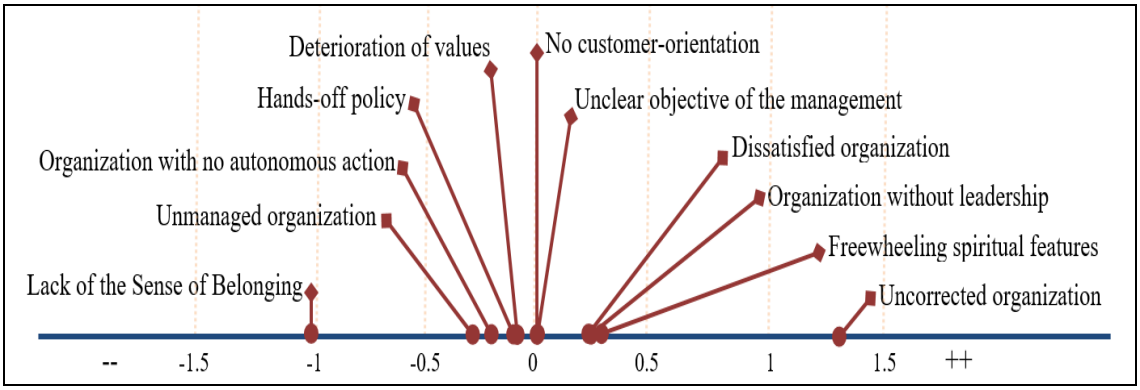


Figure 4. First derived factor

Table 13. First derived factor

Contribution Rate			16.7 %	
Cumulative Proportion Rate			16.7 %	
			Corporate Culture Variables	Variable Score
The first factor - Organizational Attribution	Liberal Profession	(+)	10.Uncorrected organization	1.314
			2.Freewheeling spiritual features	0.293
			11.Organization without leadership	0.286
			8.Dissatisfied organization	0.246
			4.Unclear objective of the management	0.093
			5.No customer-orientation	0.027
	Belonging Organization	(-)	1.Deterioration of values	-0.116
			3.Hands-off policy	-0.175
			9.Organization with no autonomous action	-0.219
			6.Unmanaged organization	-0.288
			7.Lack of the sense of belonging	-1.025

2. The second factor indicates the highest value (1.103) in “Unclear objectives of the management”, and it was inferred to prioritize the profit more than customers because of the disturbance of the management policies. In other words, there was a lack of consistency in management, such as precarious day-to-day management. As well as, it shows arrogance in the attitude and professional of the work. For these reasons, it was suggested that the second factor named as “Professional Consciousness”. Taking into account Figure 5 and Table 14, the variables that were positive including “Unclear objective of the management, Uncorrected organization, Organization without leadership, Freewheeling spiritual features, and Lack of a sense of belonging”, were considered to become more “commercial”. On the contrary, the lowest value including “Deterioration of values, Organization with no autonomous action, Unmanaged organization, Hands-off policy, Dissatisfied organization, and No customer-orientation”, were inferred to be “customer based”.

Table 14. Second derived factor

Contribution Rate			13.9 %	
Cumulative Proportion Rate			30.7 %	
			Corporate Culture Variables	Variable Score
The second factor - Professional Consciousness	Commercialism	(+)	4.Unclear objective of the management	1.103
			10.Uncorrected organization	0.748
			11.Organization without leadership	0.255
			2.Freewheeling spiritual features	0.247
			7.Lack of the sense of belonging	0.184
	Customer First	(-)	1.Deterioration of values	-0.013
			9.Organization with no autonomous action	-0.225
			6.Unmanaged organization	-0.278
			3.Hands-off policy	-0.417
			8.Dissatisfied organization	-0.474
			5.No customer-orientation	-0.494

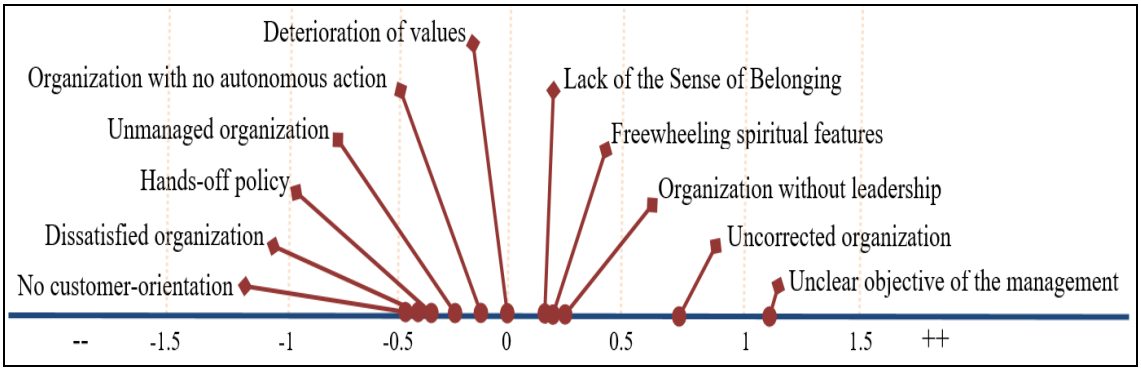


Figure 5. Second derived factor

3. The third factor shows the competing values in the three categories “Lack of a sense of belonging (0.847)”, “Hands-off policy (0.813)”, and “Organization with numerous dissatisfactions (0.465)”, and it was assumed that the cooperators could easily intrude and that those responsible may be ambiguous. Thus, it was suggested that the third factor named as “Power of Internal Control”. Taking into account Figure 6 and Table 15, the variables that were positive including “Lack of a sense of belonging, Hands-off policy, Dissatisfied organization, Unclear objective of the management, and Organization with no

autonomous action" were considered as representing an organization that is "heteronomous". And the lowest values including "No customer-orientation, Deterioration of values, Uncorrected organization, Unmanaged organization, Organization without leadership, and Freewheeling spiritual features" were inferred to be "autonomous".

Table 15. Third derived factor

Contribution Rate			13.2%	
Cumulative Proportion Rate			56.8%	
			Corporate Culture Variables	Variable Score
The third factor - Power of Internal Control	Heteronomous	(+)	7.Lack of the sense of belonging	0.847
			3.Hands-off policy	0.813
			8.Dissatisfied organization	0.465
			4.Unclear objective of the management	0.123
			9.Organization with no autonomous action	0.067
	Autonomous	(-)	5.No customer-orientation	-0.042
			1.Deterioration of values	-0.086
			10.Uncorrected organization	-0.204
			6.Unmanaged organization	-0.47
			11.Organization without leadership	-0.496
			2.Freewheeling spiritual features	-0.519

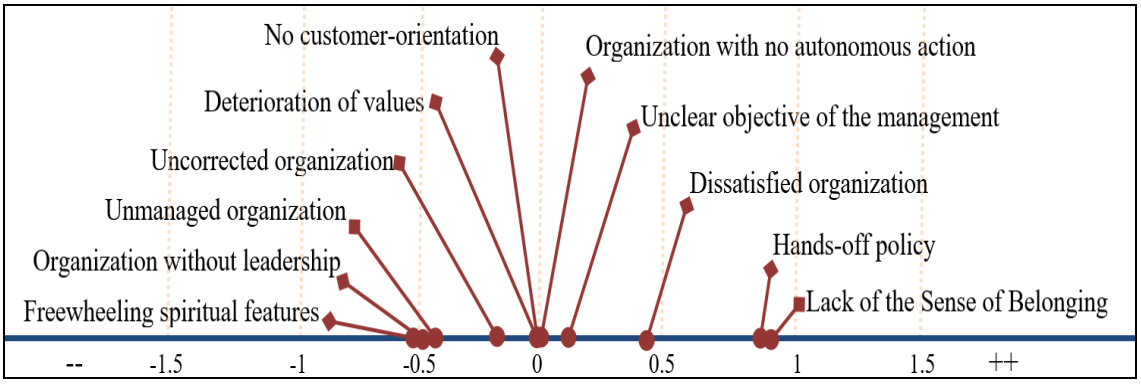


Figure 6. Third derived factor

Chapter 8. Identifying the structure of causes of organizational information security incidents.

8.1 Explanation for the use of cluster analysis

In this chapter, cluster analysis was used to assign observations to groups. Erik and Marko (2011) refers cluster analysis as "a convenient method for identifying homogenous groups of objects called clusters. Objects (or cases, observations) in a specific cluster share many characteristics, but are very dissimilar to objects not belonging to that cluster." (p.238). Thus, cluster analysis seeks to discover the number and composition of the groups, and there are several clustering methods. In this research, the hierarchal cluster analysis was used as the grouping method. The cluster is evaluating by three axes that were induced in the previous chapter. the companies in which information security incidents took place were classified in five groups as shown in Figure 7.

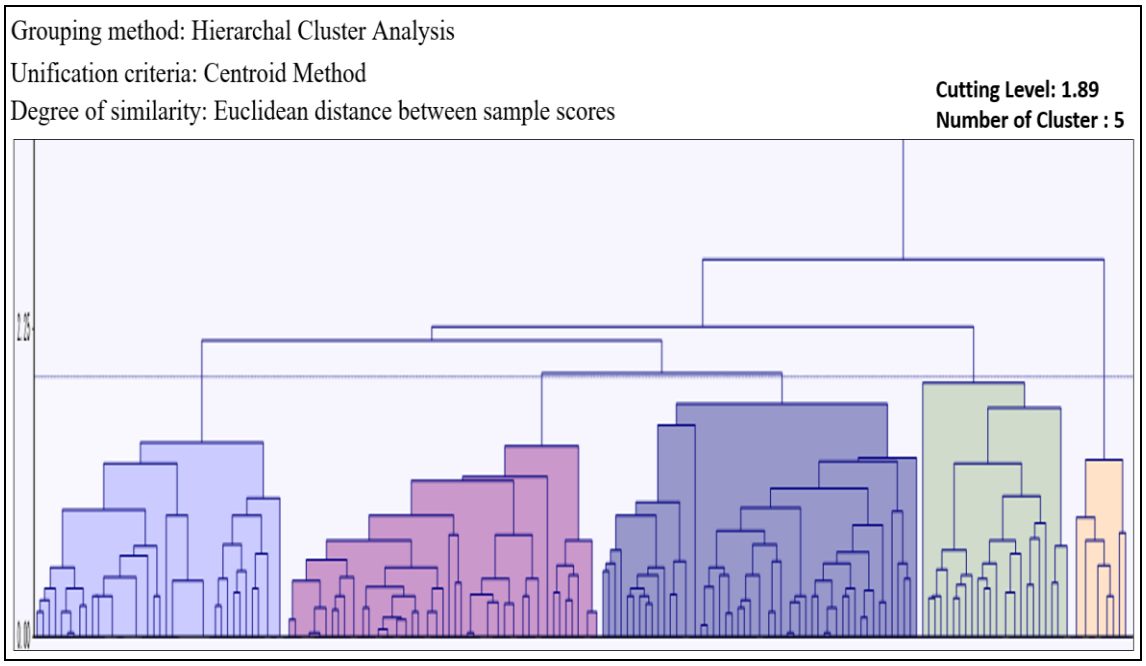


Figure 7. The output of the cluster analysis

8.2 Inducing the five clusters and the distribution of 186 organizational samples

A score was given to each factor of the sampled organizations using the technique of the hierarchical cluster analysis to group these organizations in which information security incidents took place. The distance between the centers of gravity was used as cluster unification criteria. As a result of the cluster analysis, five groups were obtained, as shown Figures 8, 9, and 10 and Table 19. The five groups were named as follows:

1. Bureaucratic self-destructive type: This group often comes under stubborn organizations such as bureaucratic organizations and large-scaled organizations. Cause of information security incidents occur through small errors.
2. None-belonging type: Information security incidents are caused by third parties such as such as contractors, due to a lack of coordination.
3. Purpose camouflage type: Information security incidents are often caused due to the lack of information security education.
4. Unguarded type: Information security incidents are caused by external factors due to lack in the information security system and fail to update it.
5. Outlaw type: An irregular group that does not belong to any of the groups above.

8.3 Features of induced clusters

8.3.1 Bureaucratic self-destructive group

This group often falls under stubborn and conservative organizations, such as bureaucratic organizations and large-scale organizations. The organizations are large, but the information security incidents occur easily through small errors. On the surface, it

seems that such as organization has security control; however, it leaves that security control up to individual autonomy, such as the employee PCs. This systematic control is weak toward the importance of the roles and the responsibilities of each organization member. Consider Figure 8. The center of the cluster for three factors was at (-0.38, -0.21, -0.11) and approximately 39 incidents were involved in this type. Most commonly, secret information was leaked because employees carried laptops containing organizational information or used unauthorized software that may contain spyware.

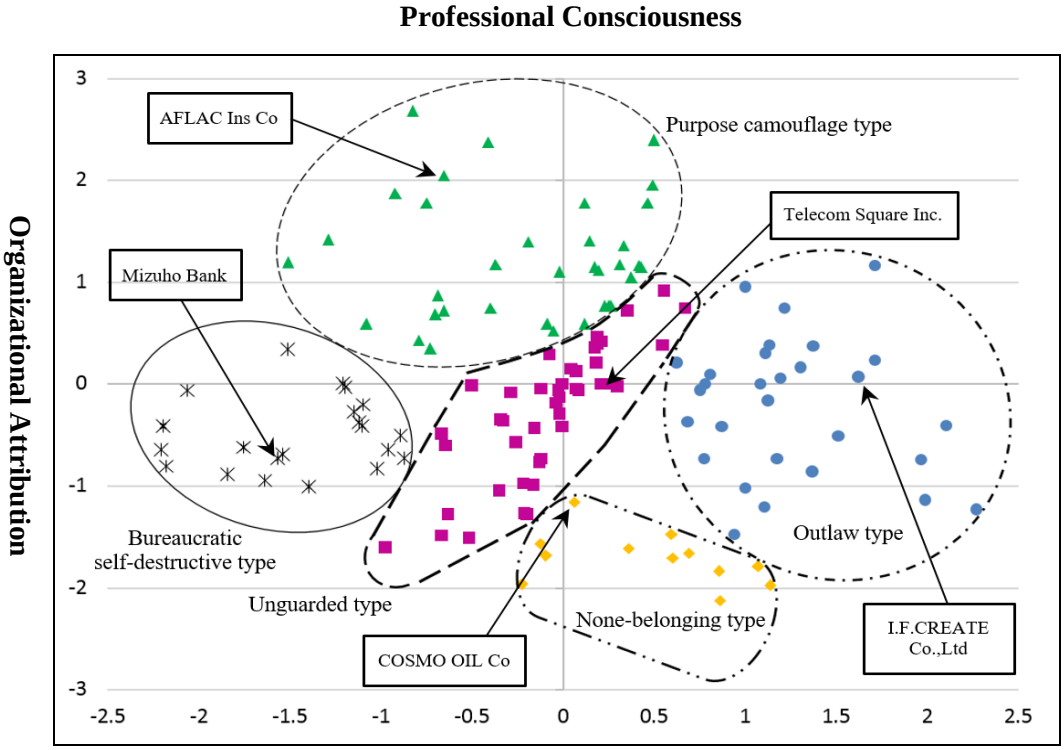


Figure 8. The First and second derived factors with five groups

8.3.2 None-belonging group

In these groups, information incidents are caused by third parties, such as contractors, due to a lack of sufficient management and coordination. The security of the organizational secret information is heteronomous: it is left to the outsourced contractors,

and therefore the information leaks when third parties (such as contractors) access the database. The center of the cluster for the three factors was at (-0.36, -0.43, 0.58) see Figure 9, involving about 17 incidents. Most often, the leakage of secret information was due to a lack of security management, access control, and surveillance of the information system. Namely, the management left personally identifiable information available to the contractors, and the information was leaked.

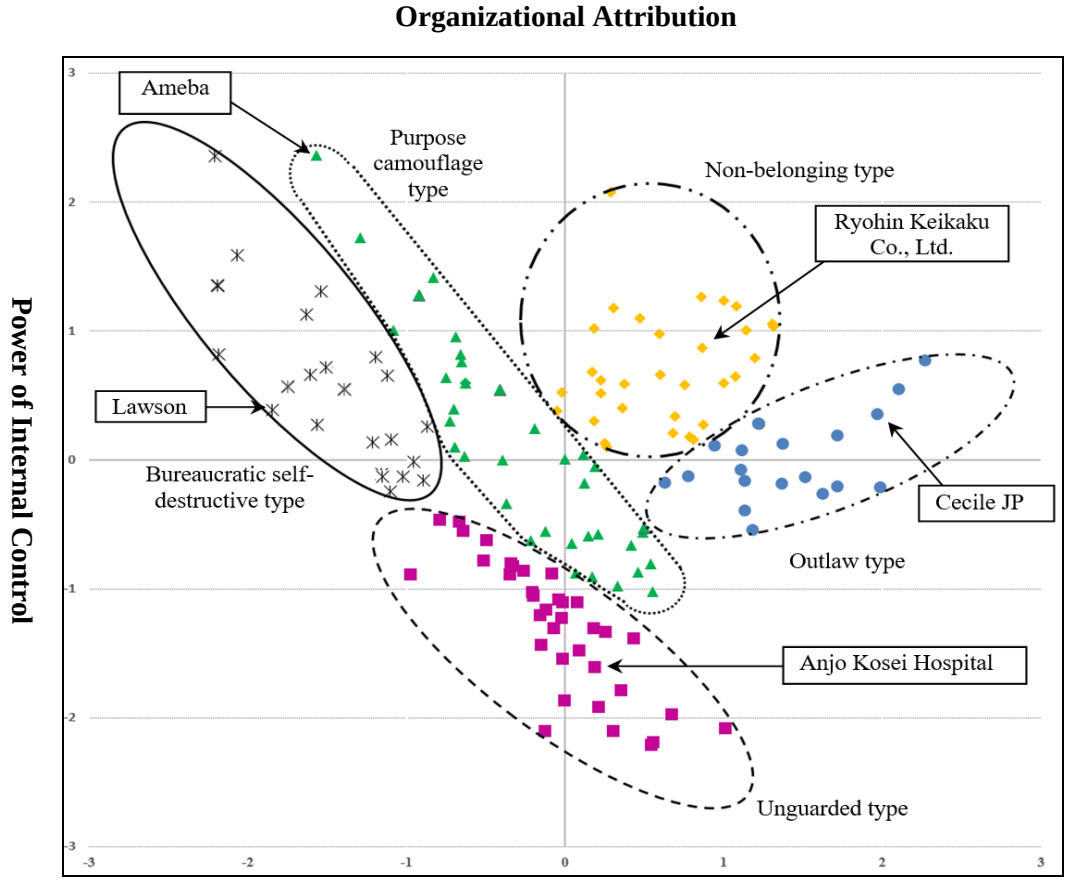


Figure 9. The First and third derived factors with five groups

8.3.3 Purpose camouflage group

In this group, information incidents are often caused by insufficient information security education. The importance of personal information is disregarded. In this type,

the possibility of higher actual damage or leakage of the organizational information might occur through social engineering, such as phishing. Such incidents occur since the importance of the responsibilities and the management of the person in charge of the secret information management is poorly recognized, and the secret information can be obtained for illegitimate uses. Thus, employees need to recognize the information's importance and be educated and trained in how to protect it. As shown in Figure 10, the center of the cluster for the three factors was at (0.095, 0.18, -0.11), with approximately 49 incidents involved. Most commonly, information was leaked because the management did not impose strict control on employees who carried out laptops or portable media devices, which contained secret information.

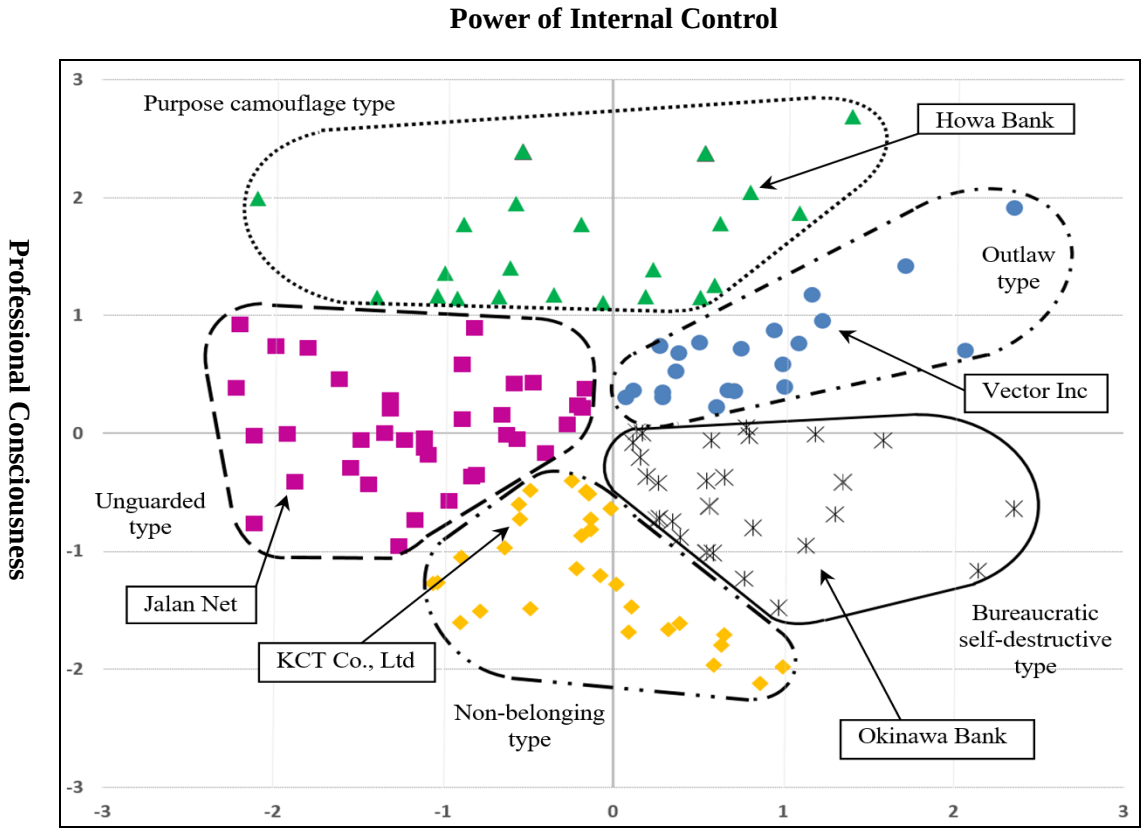


Figure 10. The Second and third derived factors with five groups

8.3.4 Unguarded group

Organizations in this group are more subject to attacks involving unauthorized access. They are apt to neglect deficiencies in their information security system and to fail to update it. As a result, information leaks are caused by external factors. This type of organization seeks social status, but does not pay sufficient attention to their clients' information security. External attacks or system vulnerabilities might cause information leaks of organizational clients. The center of the cluster for three factors was at (-0.21, -0.14, -0.15), and approximately 50 incidents were involved to this type. Most often, the leaks were due to management's failure to fulfill its responsibilities, such as performing a risk analysis, identifying vulnerability flaws, or dealing with problems caused by people within the organization.

8.3.5 Outlaw group

This is an irregular group that does not belong to any of the groups above. Furthermore, this group often starts up websites on a commercial basis. Because of the services which the organization provides through the website, these sites can easily attract those who energize their own IT techniques as criminals who take delight in people's reaction to their crimes, and those who intend to enhance their social status by successful hacking. The outlaw group fosters the private information leakage in the field of their services which they provide. The organization that provides the services entrusts the clients with the responsibility to manage private information. The center of the cluster for the three factors was at (0.064, 0.29, -0.17) and about 31 incidents were involved in this type.

8.4 Discriminant Analysis

Based upon the classification coefficients for each variable shown in Table 16, there is strong evidence of a relationship between the employee characteristics and security protocol violations. If the absolute value of a classification coefficient is greater for the security violation = 1 category is greater than the absolute value for the security violation = 0 category for a particular variable, then that independent variable likely belongs to the security violation = 1 group. For example, if an employee is relatively young, is male, and has relatively less tenure than other employees at his firm, then he is more likely to have answered yes to any of the three survey questions and to have violated security protocols. In addition, employees from departments that are older, whose jobs lean more toward managerial positions, and who are relatively less educated than their fellow employees are more likely to have violated security protocols.

Table 16. Classification function coefficients

	Security Violation=1	
	0.00	1.00
Participants' age	11.218	10.365
Participants' gender	12.494	13.042
Number of working people	0.104	-0.175
Department type	2.827	3.729
Departments' age	11.680	12.363
Job duties	1.701	1.435
Education level	13.540	13.298
(Constant)	-63.881	-63.706

Based upon the equality of group means tests shown in Table 17, it appears that three factors: Participants' age, departments' type, and departments' age contribute to the model. Additionally, participants' age and departments' age have the lowest Wilks’ lambda, which is

evidence that these two factors are better than other factors at discriminating between groups. Two groups were formed based upon three survey questions regarding various violations of security protocols. Group one is composed of individuals who answered “No” to all three survey questions. Group two is composed of individuals who answered “Yes” to at least one question regarding violation of security protocols.

Table 17. Tests of equality of group means

	Wilks' Lambda	F	df1	df2	Sig.
Participants' age	0.859	6.212	1	38	0.017
Participants' gender	0.984	0.613	1	38	0.439
Number of working people	0.950	2.020	1	38	0.163
Department type	0.918	3.398	1	38	0.073
Departments' age	0.872	5.588	1	38	0.023
Job duties	1.000	0.000	1	38	1.00
Education level	0.990	0.370	1	38	0.547

Standardized coefficients permit the comparison of variables measured on different scales Table 18, which is helpful in this case as none of the variables share similar scales. The coefficients with the largest absolute value have the greatest discriminating ability. Participants' age and departments' age are confirmed to be the best discriminators between groups.

Table 18. standardized canonical discriminant function coefficients

	Function
	1
Participants' age	-0.580
Participants' gender	0.206
Number of working people	-0.159
Department type	0.505
Departments' age	0.426
Job duties	-0.278
Education level	-0.088

Figure 11 illustrates the discriminating ability of participants' response to the question regarding being violated by a virus (Yes, No). Scatter plots of the responses with question are grouped well and are separate from each other. The discriminant analysis indicates that participants' age and departments' age are strong predictors of an individual's tendency to violate security protocols.

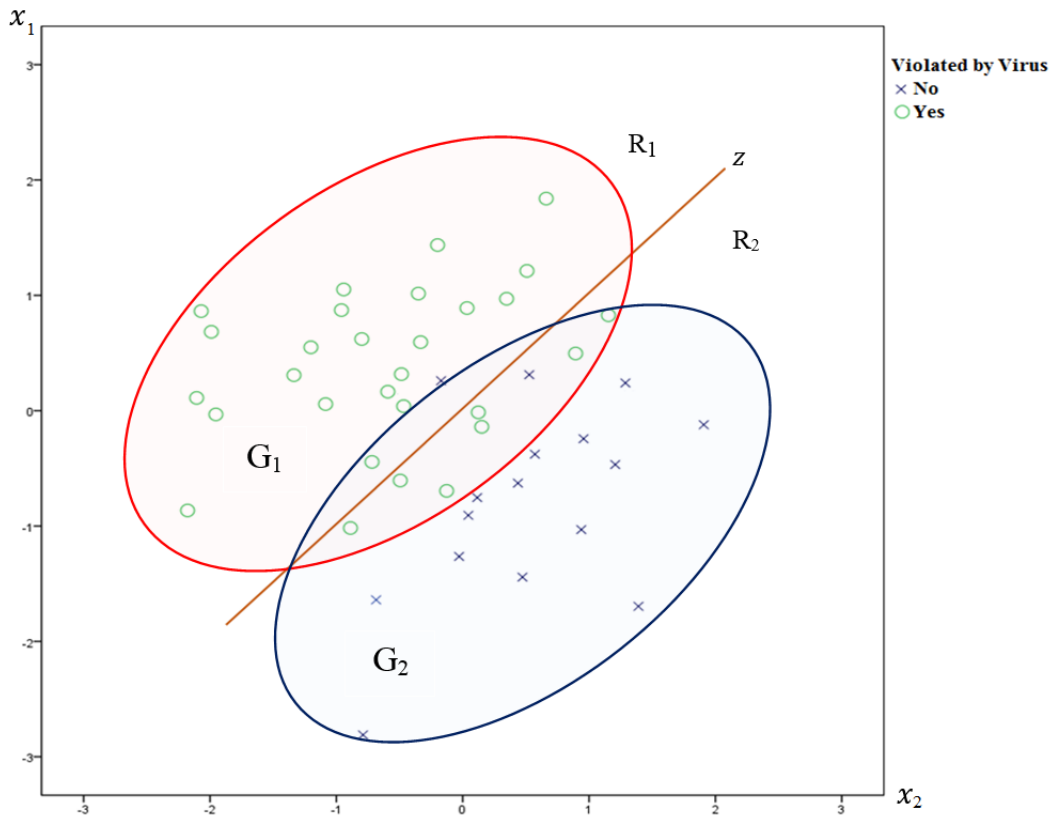


Figure 11. Discriminant between groups

Table 19. Summary of the cluster analysis for five-groups

Cluster no			1			2			3		
Cluster name			Bureaucratic self-destructive type			None-belonging type			Purpose camouflage type		
Constituent ratio			21% 39			9% 17			26% 49		
Center of the cluster			Organizational Attribution	Professional Consciousness	Internal controls	Organizational Attribution	Professional Consciousness	Internal controls	Organizational Attribution	Professional Consciousness	Internal controls
			±	±	- -	- -	±	+ +	+	-	+
			-0.38	-0.21	-0.11	-0.36	-0.43	0.58	0.095	0.18	-0.11
Cause	Risk of personal information		Leakage (35%), The leakage due to loss (31%)			Leakage (40%), loss (36%)			Leakage (36%), loss (34%)		
	Security measures	Systematic	Organizational structure (43%), development of regulations and procedures (50%)			Organizational structure (48%), Development of regulations and procedures (52%)			Organizational structure (47%), Development of regulations and procedures (49%)		
		Human	Education and training (69%), non-disclosure agreement (25%)			Education and training (76%), non-disclosure agreement (18%)			Education and training (63%), non-disclosure agreement (31%)		
		Physical	Prevention of theft (50%)			Prevention of theft (60%)			Prevention of theft (33%)		
		Technical	Access control (51%), monitoring of information systems (44%)			Access control (56%), monitoring of information systems (48%)			Access control (50%), monitoring of information systems (47%)		
	Director of employees		Management and supervision (61%), direct and command and instruction (36%)			Management and supervision (60%), direct and command and instruction (36%)			Management and supervision (56%), direct and command and instruction (43%)		
	Director of contractors		Supervision (35%)			Safety management measures (33%), trustee of Director (33%)			Safety management measures (39%), trustee of Director (39%)		
	Cause of incidents		Unauthorized access (28%), taking the PC · medium out (12%), Loss (28%), operation error (10%)			Loss (26%), Unauthorized access (15%)			Unauthorized access (32%), taking out of the PC · medium (20%)		
	Direct risk		Spending for countermeasure (43%), Losing customers (40%)			Spending for countermeasure (50%), Losing customers (33%)			Losing customers (40%), Spending for countermeasure (47%) customer churn (14%),		
	Indirect risk		Decrease of the credit (41%), a decrease in the industry (position) (40%)			Reduction of credit (49%), industry decrease of (position) (45%)			Decrease of the credit (47%), a decrease in the industry (position) (47%)		
Incidents example			Mizuho Bank Tanashi Branch Benesse Corporation. Ehime Prefecture Okayama Kurashiki Station			NTT West “FLET series” COSMO OIL Co., Ltd. Sony Sea copy Laboratories ACCA Networks			AFLAC insurance company Fujisawa firefighters Sanyo Shinpan		

Table 19 (Continued).

Cluster No			4			5		
Cluster Name			Unguarded type			Outlaw type		
Constituent Ratio			27% 50			17% 31		
Center of the Cluster			Organizational Attribution	Professional Consciousness	Internal controls	Organizational Attribution	Professional Consciousness	Internal controls
			+ +	+	+	+ +	+ +	+ +
			-0.21	-0.14	-0.15	0.064	0.29	-0.17
Cause	Risk of Personal Information		Leakage (46%), Unauthorized access (15%), loss (25%)			Leakage (40%), Unauthorized access (15%), loss (38%)		
	Security measures	Systematic	Organizational structure (48%), Development of regulations and procedures (48%)			Organizational structure (49%), Development of regulations and procedures (49%)		
		Human	Education and training (57%)			Education and training (67%)		
		Physical	Prevention of theft (38%)			Prevention of theft (50%)		
		Technical	Access control (48%), monitoring of information systems (50%)			Access control (45%), monitoring of information systems (100%)		
	Director of employees		Management Supervision (60%)			Management Supervision (57%)		
	Director of contractors		Regular grasp (43%)			Instructions of safety measures (42%)		
	Cause of incidents		Loss (17%), Virus (16%), Unauthorized access (13%), Mis-sending (13%)			Unauthorized access (18%), Loss (22%)		
	Direct risk		Spending for countermeasure (42%) Losing customers (31%)			Spending for countermeasure (47%) Losing customers (30%)		
	Indirect risk		Decrease in the industry (position) (41%), Decrease of the credit (38%)			Decrease of the credit (50%), a decrease in the industry (position) (50%)		
Incidents example			Sony's PlayStation Network Telecom Square Inc.			I.F.CREATE Co.,Ltd Happinet online		

8.5 The analysis results

Barnard (1938) suggests that the following points ought to be considered as deficiencies of the status systems and the hierarchical organization (the inverse function).

1. Deficiencies of the status system

The following points are raised as issues imposed on individuals in the status system:

- Hierarchies distort the true value of individuals in a status system.
- The circulation of the position of the elite is unfairly limited; the ability to strengthen the exclusive positions by a specific person becomes problematic.
- 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. Deficiencies of the hierarchical organization

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

Morale appearing in the hierarchical structure had decreased, and complaints have been filed for legitimate wages to be paid to a temporary staff member in spite of engaging in a significant operation in the business of Benesse Holding. This temporary staff member, using a USB, transferred the important personal information of the company externally without authorization and sold it to a name list provider.

These elements also appeared in the None-belonging type group of the second cluster. The management left personally identifiable information available to the contractors, and the information was leaked. An example of these incidents occurred in ACCA Networks and COSMO OIL Co., Ltd.

Simon (1997) considers, against the productivity of concept, which is determined by the relationship between the inputs and outputs of Taylorism, that organizations can increase

their value, prevent corporate scandals from occurring, and increase the loyalty of their employees to the organizations only when their objectives and the social value are consonant.

Generally, it can be determined as it is related to all the clusters. The information leak incidents of personally identifiable information have occurred in the unguarded type of the fourth cluster in particular because of the absence of consideration of the patients or the customers. This is entirely caused by organizational objectives and social value. The organization has failed to adhere to its social mission, and the providers themselves have attempted intrusions.

Chapter 9. Proposed assessment and improvement process of corporate culture

9.1 Impact assessment of corporate culture

Among the methods of 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 Axelrod & Cohen (2000) to organizations and clarifies both the development of corporate culture and the process of forming corporate values. agent is regarded as one that makes independent judgments and adaptively changes, and people are regarded as a type of agent, "an agent has the ability to interact with its environment, including other agents. An agent can respond to what happens around it and can do things more or less purposefully" (p.4).

The organization is composed of four elements: agents, organizational objectives, relationships between agents, and management (Hirano, 2003, p.7). 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 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, although managers are normally considered in possession of authority or power, this 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.

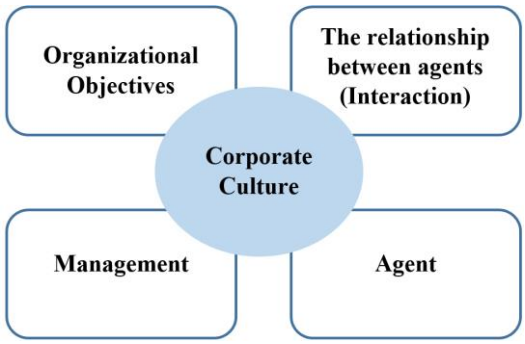


Figure 12. Corporate culture and organizational elements (Hirano, 2003, p.7).

A corporate culture impacts 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 environmental management system (ISO 14001:2004, p.2) and a privacy impact assessment “a methodology for assessing the impacts on privacy of a project, policy, programme, service, product or other initiative which involves the processing of personal information and, in consulta tion with stakeholders, for taking remedial actions as necessary in order to avoid or minimise negative impacts” (Wright & De Hert, 2012, p.5). In addition, a corporate culture aspect is defined as “the element of an organization’s activities that can interact with” the corporate culture in a similar way to an environmental management system (ISO 14001:2004, p.2).

When seeking to determine the level of information security in an organization, the essential first step is to assess 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, Schein (2009) states that "culture analysis turns out to be boring and often fruitless. The potential insights that culture can bring to you will only occur when you discover that some problem you are trying to solve or some change that you are trying to make depends very much on cultural forces" (p.77).

Within the context of cultural change and assessment, 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 might have an influence on an intended organizational change or strategic initiative. Some elements of a culture might support a change, while others could 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 might hinder the change can then be addressed (Schein, 2009).

When performing an assessment, it is important to consider the methods used for measurement. Many tools are available that can assist managers to achieve their assessment goals. One of these tools is a survey. Surveys that measure the dimensions of culture are helpful when seeking to quantify the iterations and levels of the culture (Schein, 2009). 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. The employees may be afraid that any negative responses will reflect poorly upon them, so they may have little motivation to respond honestly to the survey.

Schein (2009) explores 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 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” (p.78). The type of culture 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 determines the level of sociability and solidarity within the context of an organization’s culture. Four more cultural types emerged through this particular survey. The first is a “networked” culture, 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” (p.78) 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 attempting to establish 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 (2004) also emphasizes assessing the cultural dimensions of an organization to better facilitate its organizational objectives. To this end, a ten-step intervention was proposed (p.340-348). The purpose of the intervention was to enable "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" (p.337). 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.

In this research, a five-step process has been proposed to assess and improve corporate culture. The process is comprised of the following steps: identifying the elements and aspects that characterize the organization; assessing any change made to the corporate culture after organizational activities, establishing objectives, setting measurable targets, and measuring performance after implementing organizational activities. These steps provide a comprehensive improvement of the culture of an organization that is informative for the participants. Prior to engaging in assessment, the organization that is being assessed is first clearly explored to establish a common level of understanding. This is an effective strategic element that will be incorporated into the assessment of the IMAM Institute.

9.2 Proposed five process of corporate culture

When endeavoring to implement a new strategy or to achieve change within the context of preexisting operations, a cultural assessment is important (Schein, 2009, p.77). Employees and the culture in which they are situated influence the level of information security that is in place at an organization (Greene & D'Arcy, 2010). Given these facts, it was

essential that proposing five processes for corporate culture.

To effectively launch an assessment and to improve the corporate culture, the designer of the organization must specify which elements and aspects of the organization that may improve or degrade corporate culture. Next, the designer or planner must evaluate and suppose the change to the aspects of corporate culture. These processes are required for the assessment process of corporate culture. Using a USB memory stick to transfer information is a positive aspect such as easy to carry or use in any device; however, it also has a negative impact. When an employee carries a USB memory stick containing secret information out of corporate, the potential negative impact is the loss of confidence. For example, consider an employee in an IT department who lost a USB memory stick containing sensitive information. In this case, the employee loses the confidence of customers by failing to consider the importance of protecting their information. The employee did not uphold his responsibility to protect the customers' personal data. As a result, the department`s corporate culture is degraded. Thus, it would be necessary for the department's management to educate and discipline that employee. The above illustration is shown in the assessment process of corporate culture in Table 20. The proposed five processes are as follows:

Process 1: Specify and identify the elements and aspects of corporate culture that characterize the organization.

Process 2: Assess and presuppose the change to corporate culture after implementing organizational activities.

Process 3: Establish the objectives induced from and consistent with a new organizational policy by management.

Process 4: Set measurable targets that are achieved from the objective itself.

Process 5: Measure performance after implementing the organization's activities.

Chapter 10. Verification of the proposed assessment and improvement process for corporate culture

10.1 The results of the applied proposed assessment to IMAM employees

The five processes were made and verified for the IMAM Institute to confirm the usefulness of the proposed assessment of corporate culture as described in the previous section.

The IMAM Institute, located in Tokyo with headquarters in Saudi Arabia, is under the supervision of the Royal Embassy of Saudi Arabia. According to the IT manager in the year of 2014, the level of information security at the institute is most likely low, as information security is not taken very seriously by management. In addition, information security is still in its early stages: no information security policy exists; the security equipment is outdated; and no information security awareness programs have been launched. Access control is poor, as employees are allowed into all areas in the workplace, including the information center. However, the IT manager is working on improving information security.

After obtaining approval from the general manager, the first step in assessing the IMAM Institute was to involve the management. Engaging the managers in the assessment process was important to ensure that they participated and supported the participation of their employees “successful leaders exert their influence through a managerial and organizational culture. At the same time, they help to shape a culture, to transform” (Sergiu, 2015, p139). Further, management involvement guaranteed that the information collected would suit the intended changes or strategic initiatives that were being implemented. The managers were briefed on the assessment of corporate culture, its role in the workplace, and its influence on

information security.

After obtaining management's support to determine the proposed strategic changes or initiatives within the context of the organization, it was then necessary to quantify the existing corporate culture. The policies and procedures then in place were carefully assessed to determine their effectiveness for supporting the corporate culture as well as the level of adherence shown by the staff to aligning with the corporate culture framework already in place. Determining the effectiveness and spread of the information security environment is essential, as the next step involves directly engaging with employees and their behavior for information security.

After gaining managerial support, this study next determined the status of the corporate culture at the IMAM Institute by specifying and identifying those elements and aspects of the corporate culture that characterized the organization. The assessment of employees (agents), organizational objectives, management, and interactions between agents was the first stage on the corporate culture assessment process.

The second stage in this process was to assess the changes to the corporate culture after implementing the new organizational activities that were derived from the identified elements and aspects. During this process, the impact of information security incidents was discussed with the leader at IMAM. The agents were pinpointed as the main problem with information leaks, as they were not aware of the importance of their access to information. As a result, the employees had been disregarding the importance of information leaks.

To avoid this problem, it became essential that objectives were determined after being induced from, and being consistent with, organizational policies by management. During this

third process, objectives were established to raise employee awareness of the importance of protecting information. To achieve those objectives, measurable targets were set up.

Table 20. Assessment process of corporate culture

	Past	Present					Future
Organization	***Incidents***	***Aspect***		***Impact***	***Objectives***	***Target***	***Performance***
IMAM Inst. IT Department	An employee lost a USB device containing information (Name, Address, Contact numbers)	***Agent***	The employee has not been made aware of the importance of the job's information.	The employee disregards the information leak.	The employee is aware that the job's information should be protected from loss.	Limit the amount of confidential information stored on portable medium (USB) to only the minimum necessary. Target achievement level is 80%.	The employee takes into consideration the importance of protecting the job's information. Performance level is 25%.
		Organization's Objectives	The objectives are ambiguous, not accepted by organization members, not achievable, low on information security, etc.	The employee becomes irresponsible in their duty, does not comply with organizational policy, etc.	Management sets a policy that information should not be leaked out of the organization.	Each member of the IT department will be required to read and understand the information security policy. Target achievement level is 100%.	The employee contributes to his department, and has awareness of deparment strategies. Performance level is 70%.
		Management	The management has not invested in equipment, training programs or awareness activities for employees.	Unwanted and unexpected events which suddenly occur in the organization are ignored or left alone.	Management invests in the budget and ensures policies are well-known and understood.	Each member of the IT department will be required to attempt training programs, and frequently measure the response of staff members using awareness programs. Target achievement level is 100%	Management takes secret information seriously, and creates the necessary awareness and training programs. Performance level is 90%.
		Interaction between Agents	Management and employees do not share organizational values.	Shared organizational values degrade, collapse, etc.	Shared organizational values will be improved.	Information on unwanted or unexpected events is provided through the hierarchy, via interaction between agents. Target achievement level is 100%.	Information on unwanted or unexpected events are provided. Performance level is 20%.

For example, the amount of secret information stored on portable devices, such as USB memory sticks, was limited to the absolute minimum. After completing this fourth process, and in order to assess its effectiveness, it was then necessary to measure performance once these organizational changes were made.

The case of the IMAM Institute illustrates how a corporate culture assessment can be significant for improving the corporate culture and reducing information security incidents.

10.2 How to improve the organizational defect which has incidents

To improve organizational defect and to prevent information security incidents from taking place in the future in the workplace level, it is important to improve the corporate culture through policies at the organization level which are not highly dependent on a compliance system. To maintain the social trust of an organization by preventing these incidents, and to avoid deterioration of the management environment, it is necessary not only to build an internal control system with top-down compliance, but also to improve the corporate culture in the workplace by exerting leadership at the management or the workplace level.

Within the context of organizations, the maintenance of information security is a key element in protecting organizations from various sources of harm. An organization’s members are the most significant source of information security incidents. Members and their behavior within the systems of the workplace pose the greatest threat to information security technology because of their greater access to and understanding of the importance of information security. Often, members have a lower understanding of the importance of

information security than their level of access, placing organizations at risk.

Organizations that 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, which lowered people's morale, in addition, it increased the injustice and the unethical behaviors of organization (Mitchell, 2001, p.29). To prevent from these injustice and unethical behavior of companies; it would be insufficient if only the comprehensive 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. The shortcomings were the disparities in the distribution of wages, honor and prestige among different positions could lowered employee's morale as Barnard (1938) suggestion. The wage system is problematic in terms of labor motivation and organizational efficiency; the wage system has a problem from the viewpoint of information security incidents. 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.

To mitigate the potential threats associated with poorly managed information security, it is important for organizations to establish policies that will ensure the security of information, whether within the internal systems of the organization, or online. To support a strong information security environment, it is imperative that organizations assess their corporate culture. This includes an evaluation of agents, objectives, management, and interactions between agents, as well as their ability and willingness to implement information

security measures. Through ongoing assessments, the strengths and weaknesses may be noted in real time, with emerging threats identified sooner, allowing for a more expedient response to mitigate the threat. Information security incidents are a complex element in modern business that must be supported across the entirety of organization to ensure that information security is maintained.

10.3 The results of applying the five process

The results of applying the five process for the first group of the five groups have been determined through cluster analysis; the bureaucratic self-destructive type, since the systematic control is weak toward the importance of the responsibilities of each organization members. The established objective could be: Management sets a policy that information should not be leaked out of an organization. The targets could be as follows: Each employee of the organization will be required to read and understood the information security policy; performance could be measured by the employees' contribution to the organization and awareness of organizational strategies. The findings indicate that all organizations' employees shall be made aware of their responsibilities for maintaining effective access controls, and the organization shall launch appropriate employee training programs about their functions and work duties. Moreover, identifying physical perimeters and barriers, along with physical access controls and working procedures, should protect buildings, offices, and delivery and loading areas against unauthorized access. In addition, special guidance should be provided for security against natural disasters.

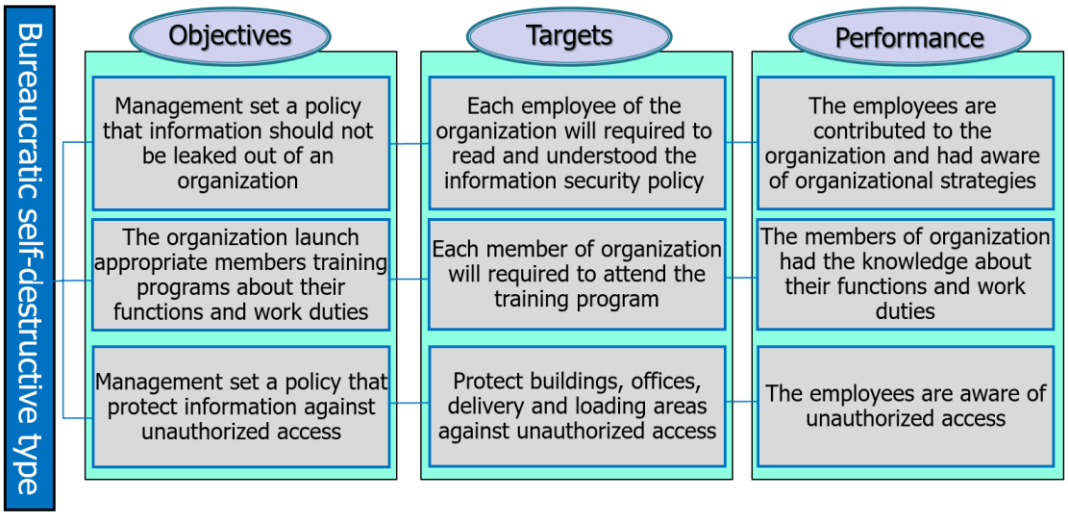


Figure 13. Bureaucratic self-destructive type improvement

For the second group, none-belonging type, organizations left information to the outsourced contractors, and therefore the information leaks when third parties access the database. Security responsibilities should be considered when hiring contractors or temporary employees. For example, background verification checks and terms and conditions of employment, including signed agreements of security roles and responsibilities, need to be addressed. In addition, updating access rights and emphasizing the continuing obligations under privacy laws to contractors to protect the organization's assets should be part of the process of changing or terminating contractors. The objectives could be stated as follows: security responsibilities should be considered when hiring contractors or temporary employees. The targets could be background verification checks and terms and conditions of employment, including signed agreements. Performance could be determined by employee's suitability to perform the required duties and responsibilities within an organization.

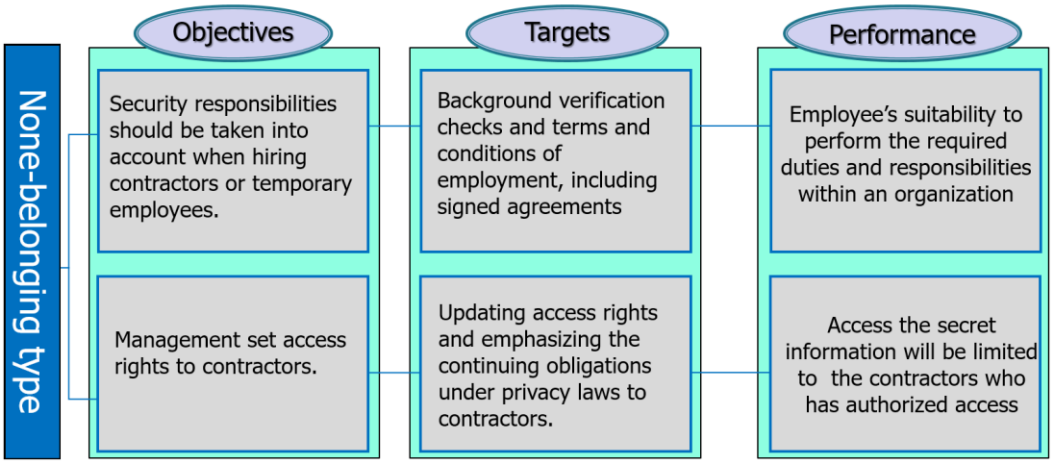


Figure 14. None belonging type improvement

In the purpose camouflage type, since the majority of incidents occurred due to carried out laptops or portable media, which is mostly attributed to insufficient information security education, an organization's employees, contractors, or temporary employees shall become aware of the information security policy, and these policies shall be defined, published, and communicated to all employees. In addition, all employees shall complete an appropriate updated awareness program and receive training. The objectives could be as follows: the management should impose strict control on employees who carry out laptops or portable media devices containing secret information. The targets could be to apply strict control to all employees and limit the amount of secret information stored on portable devices, such as laptops or USBs. Performance could be assessed as the importance of the responsibilities, and the management of the person in charge of the secret information is recognized.

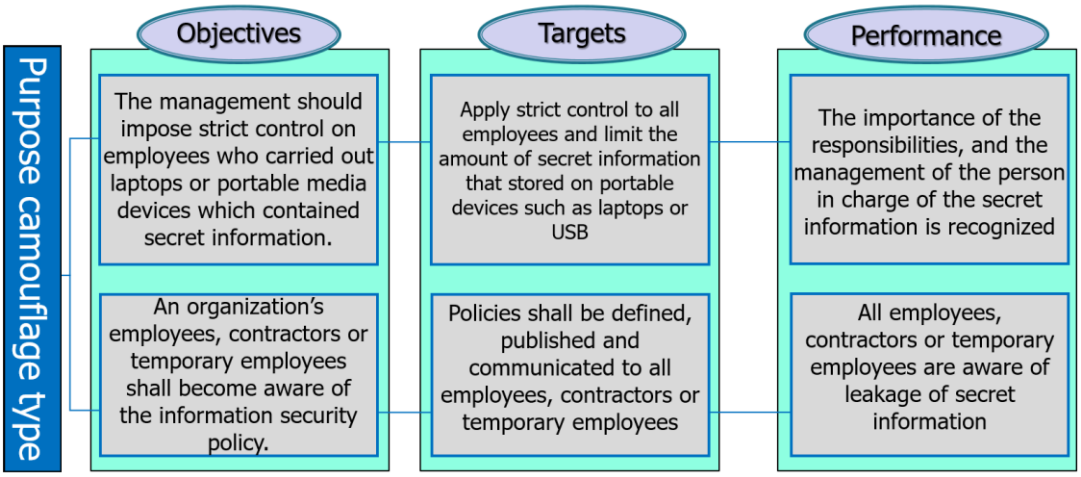


Figure 15. Purpose camouflage type improvement

For the unguarded type, the leaks were due to management's failure to fulfill its responsibilities, such as performing a risk analysis and identifying vulnerability flaws. The objectives could be stated as follows: Management should ensure that information is protected against external attacks. For example, organizational requirements to control the access of information processing facilities should be established and documented in an access control policy. Access to the networks services should be limited to authorized users. In addition, to ensure that information is protected against external attacks, technical vulnerabilities should be patched, and software installation on organizational systems should be restricted. Furthermore, antimalware software, IPS, and Firewall are required. The targets could be stated as follows: Technical vulnerabilities should be patched, and software installation on organizational systems should be restricted. In terms of performance, information on unwanted or unexpected events is provided.

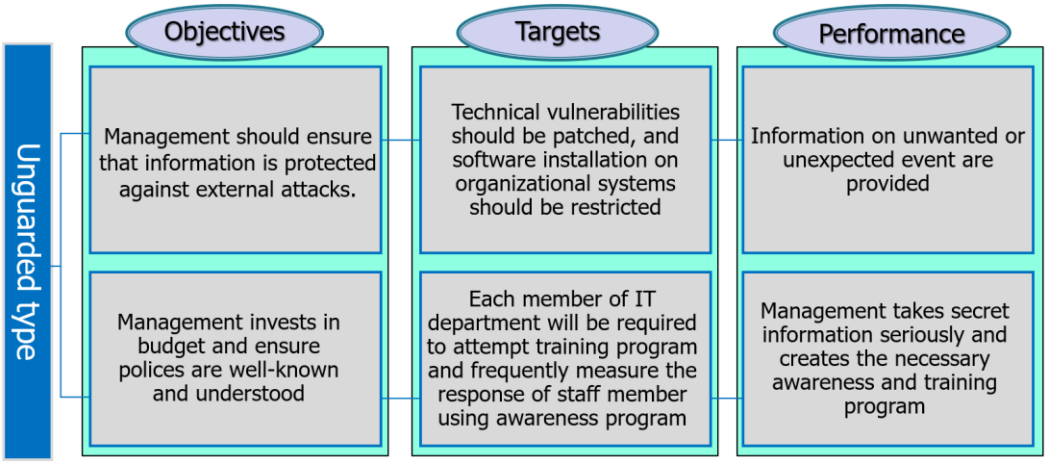


Figure 16. Unguarded type improvement

For the fifth group, the outlaw type, the objectives could be stated as: Management should establish and administer privileged user accounts in accordance with role-based access. For the targets: Limit the access to secret information in accordance with the access control. Finally, for performance: Employees are familiar with and understand the access policies, such as secure log on and password management.

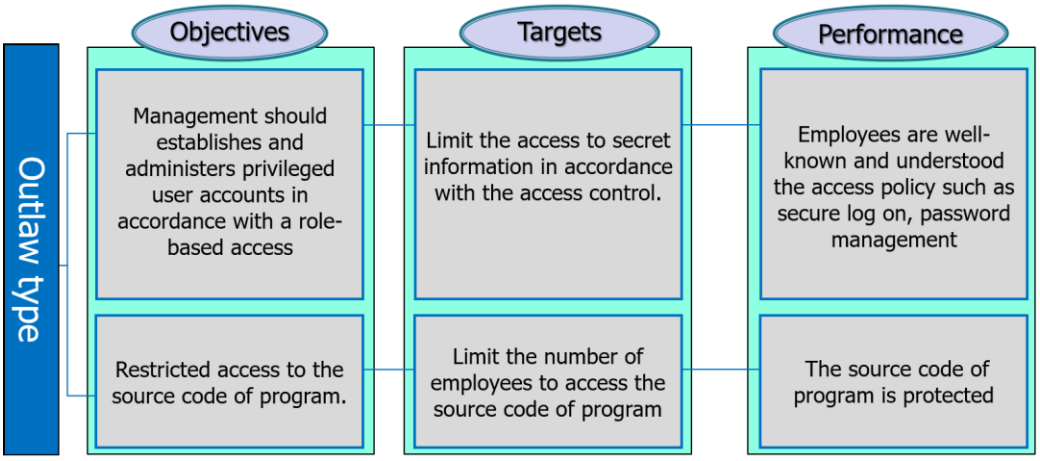


Figure 17. Outlaw type improvement

Chapter 11. Conclusion

The occurrence of information security incidents within an organization has become a highly important topic. Information security incidents are linked to both people and technology; however, while security technology itself is targeted by people, people are influenced by corporate culture, which might in turn significantly affect information security.

In this research, eleven main factors were induced. By utilizing the questionnaire data, this research investigated how such culture in a general workplace is specified by the factors which can be operated by the management's actions, 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 behaviors, including scale, moral leadership, and other single indicators, have a powerful influence on corporate culture. 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.

This research collected data on 186 samples of organizations where information security incidents had occurred in the past, where it was verified that similar scandals and incidents had similar causes, arising from social values or corporate culture. The research produced primary findings. First, three axes were used to identify the causes of information security incidents: organizational attribution, professional consciousness, and power of internal controls. Second, regarding the mechanisms behind information security incidents, five clusters were derived by analyzing the sampled organizations where information security

incidents had occurred in the past. The five clusters found were classified as the bureaucratic self-destructive type, the none-belonging type, the purpose camouflage type, the unguarded type, and the outlaw type.

In this research, the mechanisms of information security incidents were identified, and the main factors concerning information security incidents were induced. And the relationship between aspect and impact of the incidents was identified. Furthermore, five-processes method has been proposed in order to improve organizational defects. The effectiveness of the five-process method was verified, both for the IT department at the Saudi Arabian Embassy in Japan and the Arabic Institute at IMAM Branch of Saudi Arabian University.

References

Alfawaz, S., Nelson, K., & Mohannak, K. (2010). Information security culture: A behavior compliance conceptual framework. Australian Computer Society, *Proceedings of the Eighth Australasian Conference on Information Security*. 105,47–55.

Alnatheer, M., Chan, T., & Nelson, K. (2012). Understanding and measuring information security culture. *Proceedings of Pacific Asia Conference on Information Systems*. 144.

Axelrod, R., & Cohen, M. (2000). *Harnessing complexity: Organizational implications of a scientific frontier*. New York: Basic Books. ISBN 0-465-00550-0

Barnard, I. (1938). *The functions of the executive*. Cambridge, MA: Harvard University Press.

Churchill, G. (1979). A paradigm for developing better measures of marketing constructs. *Journal of Marketing Research.* 16(1), 64-73.

Coles-Kemp, L., & Theoharidou, M. (2010). Insider Threat and Information Security Management. *Insider Threats in Cyber Security: Advances in Information Security*. Springer Science, 45–71.

Da Veiga, A. (2015) The influence of information security policies on information security culture: illustrated through a case study. *Proceedings of the ninth international symposium on human aspects of information security & assurance.* 22–33.

Da Veiga, A., & Eloff, J. H. (2010) A framework and assessment instrument for information security culture. *Computers & Security*. 29(2), 196–207.

Deal, T. E., & Kennedy, A. A. (1982). *Corporate cultures: The Rites and Rituals of Corporate Life*. Boston, MA: Addison-Wesley.

DLP *Information leakage news [情報漏えいニュース]*. Antitheft. Retrieved from http://blog.livedoor.jp/antitheft/

Donahue, S. E. (2011). *Assessing the Impact that Organizational Culture has on Enterprise Information Security Incidents.* PHD thesis. MN: Capella University

Dzazali, S., & Zolait, A. H. (2012). Assessment of information security maturity: An exploration study of Malaysian public service organizations. *Journal of Systems and Information Technology*. 14(1), 23–57.

Environmental Management System – Requirements with guidance for use. ISO 14001:2004.

Erik, M., & Marko, S. (2011). *A concise guide to market research*. Springer-Verlag Berlin Heidelberg.

Gebrasilase, T., & Lessa, L. F. I. (2011). Information security culture in public hospitals: The case of Hawassa Referral Hospital. *The African Journal of Information Systems*, 3(3), 72–86.

Gerbing, D., & Anderson, J. (1988). An updated paradigm for scale development incorporating unidimensionality and its assessment. *Journal of Marketing Research.* 25(2), 186-192.

Greene, G., & D'Arcy, J. (2010). Assessing the impact of security culture and the employee-organization relationship on IS security compliance. *5th Annual Symposium on Information Assurance*. 42–49.

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2010). *Multivariate data analysis* (7th ed.). N.J: Pearson Prentice Hall.

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

Hirano, M. (2003). *The McKinsey anthology [マッキンゼー 組織の進化]* 、ダイヤモンド社.

Hobson, D. (2008). The real cost of a security breach. *SC Magazine*, Retrieved from https://www.scmagazine.com/the-real-cost-of-a-security-breach/article/554815/

Hofstede, G. (2010). *Culture and organizations: Software of the mind*. NY: McGraw-Hill.

Hoshino, T., Arai, K., Hirano, S., & Yanagisawa, H. (2008). An empirical analysis of organizational climates of misconduct [組織風土と不祥事に関する実証分析] 、*一橋経済学*、*Hitotsubashi economics*, 2(2), 157–177. Retrieved from https://hermes-ir.lib.hit-u.ac.jp/rs/handle/10086/15869

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, 43(4), 615–660.

ISO/IEC. (2013). *Information technology – Security techniques – Information security management systems – Requirements*. ISO/IEC 27001:2013. British Standards Institute.

Kayworth, T., & Whitten, D. (2010). Effective information security requires a balance of social and technology factors. *MIS Quarterly Executive*, 9(3), 163-175

Kline, R. B. (2011). *Principles and practice of Structural Equation Modeling* (3rd.). New York: Guilford Press.

Koufteros, X. (1999). Testing a model of pull production: a paradigm for manufacturing research using structural equation modeling. *Journal of Operations Management.* 17(4), 467-488.

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

Laybats, C., & Tredinnick, L., (2016). Information security. *Business Information Review*. 33(2), 76-80.

Lim, J. S., Ahmad, A., Chang, S., & Maynard, S. (2010). Embedding information security culture emerging concerns and challenges. *PACIS 2010 Proceedings.* Paper 43. 463–474.

Lu, C., Lai, K., & Cheng, T. (2007). Application of structural equation modeling to evaluate the intention of shippers to use Internet services in liner shipping. *European Journal of Operational Research*. 180(2), 845-867.

Mano, O. (1989). The Meaning of the Concept of Lateral Organization in C.I.barnard's Theory [バーナード理論におけるLateral Organizationの位置]、*經濟學研究*、 *Economic Studies, 39(1): 1-7.*

Mitchell, L.E. (2001). *Corporate irresponsibility: America's Newest Export*. New Haven: Yale University Press.

Miyoshi, H. (2005). Organizational culture and organizational change to enhance the quality of the organization [組織のクオリティを高める組織風土・体質変革] 、*クオリティマネジメント、56 (9): 18-23.*

Nosworthy, J. D. (2000). Implementing information security in the 21st century: Do you have the balancing factors? *Computers & Security.* 19, 337–347.

Oehri, C., & Teufel, S. (2012). Social media security culture. *Information Security for South Africa (ISSA).* 1–5.

Padayachee, K. (2012). Taxonomy of compliant information security behavior. *Computers & Security.* 31(5), 673–680.

Pallant, J. (2005). *SPSS survival manual: A step by step guide to data analysis using SPSS for Windows* (Version 12). Crows Nest NSW, Australia: Allen & Unwin.

Ponemon Institute. (2011). *2011 Cost of Data Breach Study: Japan.* Retrieved from http://www.ponemon.org/local/upload/file/2011_ CODB_JP_Final_5.pdf

Privacy Rights Clearinghouse. (2010). *500 million sensitive records breached since 2005.* Retrieved from https://www.privacyrights.org/blog/500-million-sensitive-records-breached-2005.

Scan Net Security. Retrieved from http://scan.netsecurity.ne.jp/category/incident/2014/01/

Schein, E. H. (2009). *The corporate culture survival guide*. San Francisco: Jossy-Bass.

Schein, E.H., (2004). *Organizational Culture and Leadership* (3rd ed.). San Francisco, CA: Jossey-Bass.

Security NEXT, Retrieved from http://www.security-next.com/monthlyarchive.

Sergiu, G. (2015). Developing the organizational culture. *Revista De Management Comparat International*, 16(1), 137-143. Retrieved from https://search.proquest.com/docview/1708137561?accountid=142908

Shover, N., & Hochstetler, A. (2002). Cultural explanation and organizational crime. *Crime, Law, and Social Change*. 37, 1–18.

Simon, H. (1997). *Administrative Behavior: A study of Decision-Making Processes in Administrative Organizations* (4th ed.). New York: Free Press. ISBN-13: 978-1-4391-3606-5 (eBook).

Talib, S., Clarke, N. L., & Furnell, S. M. (2011). Establishing a personalized information security culture. *International Journal of Mobile Computing and Multimedia Communications* (IJMCMC). 3(1), 63–79.

Taylor. F. (1911). *The principles of scientific management*. New York, NY: Harper & Brothers.

Vacca, J. R. (2013). *Computer and information security handbook* (2nd ed.). MA: Elsevier.

Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security*. 29(4), 476–486.

Verton, D. (2000). Companies aim to build security awareness. *Computerworld*. 34(48), 24. Retrieved from http://www.computerworld.com/article/2589214/it-skills-training/companies-aim-to-build--security-awareness.html

Vroom, C., & Von Solms, R. (2004). Towards information security behavioral compliance. *Computers & Security*. 23(3), 191–198.

Whitman, M. E., & Mattord, H. J. (2011). *Principles of information security* (4th ed.). Boston, MA: Course Technology.

Wright, D., & De Hert, P. (2012). *Privacy impact assessment: Law, Governance and Technology Series*. New York: Springer Science and Business Media.

APPENDIX (A): Survey Instrument

QUESTIONNAIRE

Dear Participant,

I am Abdullah Almubark, a PhD student at Tokyo University of Information Sciences, working toward a doctorate degree in informatics. You are invited to take part in a research study which focuses on investigating information security incidents in your organization.

To participate, please read the following:

Purpose: is to provide: 1) insights into the influence of corporate culture factors on information security incidents.

Procedure: your participation will involve completing the enclosed questionnaire, which comprises some background questions, and statements about your perception of information security incidents. This study will take approximately 10-15 minutes.

Potential benefits: your participation will help to understand the influence of corporate culture factors on information security incidents at your particular organization.

Confidentiality: confidentiality of the information you provide is assured. The questionnaire forms do not require you to identify yourself, and only grouped data will be used in the research. The information collected will be only used for the purpose of this study.

Your cooperation in participating in this research is deeply appreciated.

Yours sincerely

Abdullah Almubark

Tokyo University of Information Sciences

Graduate School of Informatics

APPENDIX (A): Survey Instrument in Japanese

アンケートにご協力お願いいたします

皆様へ
私はアブドラ　アルムバラクと申します、東京情報大学で博士課程学生をしています。

現在、このアンケートは研究中の「情報セキュリティインシデントと組織との関係について」のデータを得るために皆様方にデータ採りの協力をお願いする次第です。

なお、このアンケートすべては統計処理され、調査以外の目的には一切使用し致しません。
このアンケートは、約 **10〜15** 分かかります。

皆様方の参加は、情報セキュリティインシデントと組織との関係についてを理解するのに役立ちます。

この研究に参加することにご協力を感謝致します

アブドラ　アルムバラク

東京情報大学

博士後期課程

APPENDIX (A): A questionnaire for the IT department of the IMAM Institute (Part 1)

1. **Your age (年齢):**
   □ 20 and less □ 21 – 30 □ 31 – 40 □ 41 – 50 □ 51 – 60
   □ More than 60
2. **What is your gender (男性、女性)**
   □ Male (男性) □ Female (女性)
3. **How many people are working in the organization? 所属組織の従業員数**
   □ 20 and less □ 21–99 □ 100–499 □ More than 500
4. **Which department that you work? (所属部門)**:
   □ Financial (財務部) □ Education (教育部門) □ IT □Other (その他) _____
5. **Department age (現在の業務の経験年数):**
   □ 0–3 year's □4–6 year's □More than 7 year's □Do not know
6. **Job duties (職責):**
   □Management (経営者、上級管理者) □ Manager (管理者) □Leader (リーダー)
   □Employer (正式の従業員) □ Contractor (契約社員)
   □Part-timer (パート・アルバイト) □ Third vendor's Employer (サードベンダの従業員)
7. **Your graduate school (卒業):**
   □Graduate School of university (大学院) □university, collage (大学、短大、専門学校)
   □High School (高校) □Other (その他)
8. **Have you been violated by a virus to your computer?**
   あなたのパソコンはウイルスに罹ったことがありますか。
   □ **Not have (ない)** □ **Have (ある)**
9. **Have you looked into a password of another person?**
   あなたは他人のパスワードを覗き込んだことがありますか。
   □ **No I have not (ない)** □ **Yes I Have (ある)**
10. **Have you been shared your password with another person?**
    自分のパスワードが他人に知られたことがありますか。
    □ **No I have not (ない)** □ **Yes I Have (ある)**

APPENDIX (A): A questionnaire for the IT department of the IMAM Institute (Part 2)

Table 21. Questionnaire regarding culture of fraud and neglect of violation in the workplace Used from Hoshino, et.al (2008, p.163, Table 1.) 職場での不正・違反放置の風土

	質問項目 Question Items	ない None	あまりない Mostly None	たまにある Occasionally	ときどきある Sometime	頻繁にある Frequently
1	Did you ever disobey the basic rules in your workplace? あなたの職場では基本的なルールが破られることがありますか。					
2	Did you ever do unreal reports in your workplace? あなたの職場では虚偽報告のなされることがありますか。					
3	Have you seen the performance of dishonest means with respect to important decisions in the past? 重要な意思決定（人事を含む）に関して、意図的に不正（非倫理的）な手続きがとられたのをあなたは見たことがありますか。					
4	In your workplace, did your manager ever neglect the fraud even knowing them? あなたの職場では、管理者が不正を知りながら放置していることがありますか。					
5	In your workplace, did your manager ever instruct you to conceal the fraud? あなたの職場では、管理者が不正の隠蔽を指示することがありますか。					
6	Do you have an atmosphere that earns a profit, even by illegal act? あなたの職場には、違法行為をしてでも利益を獲得しようという雰囲気がありますか。					

Table 21. (continued).

7	For problems such as illegal act happened in other organizations, do you have an atmosphere that your organization would not take the same actions? 他社（他の組織）が問題とされることなく違法行為をしているときは、自社（自分の組織）も同様にしてもかまわないという雰囲気があなたの職場にはありますか。					
8	Does an illegal act done by the group of decision making in your workplace? あなたの職場では集団（複数の人間）の意思決定によって不正行為がなされますか。					

Table 22. Questionnaire regarding trust toward the workplace
Used from Hoshino, et.al (2008, p.163, Table 1.) 職場における信頼

Question Items 質問項目		そう思わない Disagree	あまりそう思わない Tend to disagree	どちらともいえない Neither agree nor disagree	ややそう思う Somewhat agree	そう思う Agree
9	Do you think the coworker can collaborate closely in your workplace? あなたの職場では、同僚同士が分け隔てなく協力的ですか。					
10	Do you think the information transfer between members is performed widely and smoothly in your workplace? あなたの職場では、成員間の情報伝達が広く円滑に行われますか。					
11	Do you think your co-worker reliable at work? あなたの同僚は仕事の上で信頼できますか。					

Table 22. (continued).

12	Do you think your manager reliable on work? あなたの上司は仕事の上で信頼できますか。					
13	If you put priority on doing the right thing, will your manager and co-worker support you? あなたが正しいことを率先してすると、あなたの上司や同僚は支持してくれますか。					

Table 23. Questionnaire regarding sectarian behavior
Used from Hoshino, et.al (2008, p.163, Table 1.) 派閥的行動

Question Items 質問項目		そう思わない Disagree	あまりそう思わない Tend to disagree	どちらともいえない Neither agree nor disagree	ややそう思う Somewhat agree	そう思う Agree
14	Do some people form a strong conspiracy in your workplace? あなたの職場では一部の人たちが強固な結託を形成していますか。					
15	In your workplace meeting, do some people work together to get a favorable resolution with complicity? あなたの職場の会議では、一部の人たちが陰で共謀して有利な決議を得ようとしますか。					
16	Is it difficult for you to propose an opposite opinion against the members of mainstream faction in your workplace meeting? あなたの職場の会議では、主流派閥の成員に対する反対意見が言いにくいですか。					

Table 23. (continued).

17	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? あなたの職場では、有力な派閥（仲良しグループ）に所属しない個人は、仕事上不利な取り扱いや嫌がらせを受けますか。					
18	Are there any "escape goat" (people to sacrifice) in your workplace, so that anything inconvenient can be attributed to them? あなたの職場では少数のエスケープゴート（犠牲となる者）が作り上げられて、都合の悪いことはそれに負わせますか。					
19	Are the people surrounded by the yes-man subordinate leaders of your organization or workplace? イエスマンの部下で周囲を固めた人間が、あなたの組織や職場を牛耳っていますか。					
20	Does the subordinate who does not do the present (gift) for the manager become disadvantageous by promotion in your workplace? あなたの職場では上司に対する付け届けをしない部下は昇進で不利になりますか。					

Table 23. (continued).

21	Are the individuals who actively speak sound arguments labeled as "problem child", and ignored or shunned in the workplace? 積極的に正論を発言する個人は「問題児」などのレッテルを貼られて、職場内で無視または敬遠されますか。					
22	Are the claims of some of members almost all accepted regardless of its content? あなたの職場では、一部の成員の主張はその内容にかかわらずほとんど受入れられますか。					

Table 24. Questionnaire regarding belonging scale
Used from Hoshino, et.al (2008, p.163, Table 1.) 属人尺度

Question Items 質問項目		そう思わない Disagree	あまりそう思わない Tend to disagree	どちらともいえない Neither agree nor disagree	ややそう思う Somewhat agree	そう思う Agree
23	In a face-to-face meeting with the opponent, it happened that you could not express your dissenting opinion. 相手の対面を重んじて、会議やミーティングなどで反対意見が表明されないことがある。					
24	In a meeting, even the same proposal will have different result in being passed or not depending on the proponent. 会議やミーティングでは、同じ案でも、誰が提案者かによってその案の通り方が異なることがある。					

Table 24. (continued).

25	When trouble occurs, the atmosphere there is more of "whose responsibility it is" than of "what the cause is". トラブルが生じた場合、「原因が何か」よりも「誰の責任か」を優先する雰囲気がある。					
26	People are evaluated more from likes and dislikes than the way they do work. 仕事ぶりよりも好き嫌いで人を評価する傾向がある。					
27	The priority of work is often decided by who has requested. 誰が頼んだかによって、仕事の優先順位が決まることが多い。					

Table 25. Questionnaire regarding moral leadership
Used from Hoshino, et.al (2008, p.163, Table 1.) 道徳的リーダーシップ

Question Items 質問項目		そう思わない Disagree	あまりそう思わない Tend to disagree	どちらともいえない Neither agree nor disagree	ややそう思う Somewhat agree	そう思う Agree
28	In your workplace, does a manager emphasize restraint of the injustice definitely? あなたの職場では、経営者・管理者が不正の抑止を明確に強調していますか。					
29	Are the managers in your workplace behaving as the moral model for others? あなたの職場の経営者・管理者は、他の成員の模範となるような倫理的行動をしていますか。					

Table 25. (continued).

30	Have the managers in your workplace a strong sense of mission? あなたの職場の経営者・管理者は強い使命感を持っていますか。					

Table 26. Questionnaire regarding leadership in the workplace level
Used from Hoshino, et.al (2008, p.163, Table 1.) 職場レベルでのリーダーシップ

Question Items 質問項目		そう思わない Disagree	あまりそう思わない Tend to disagree	どちらともいえない Neither agree nor disagree	ややそう思う Somewhat agree	そう思う Agree
31	Does the top of your workplace put entrenchment in the first place instead of self-sacrifice? あなたの職場のトップは自己犠牲よりも保身を第一に考えますか。					
32	When you are confused in a judgment, will your manager give appropriate Legal instructions for the entire workplace? あなたが判断に迷ったとき、あなたの上司は職場全体にとって適切な合法的指示をしてくれますか。					
33	Does your manager brandish their power to the subordinate one hand, but behave obediently to people in the upper position? あなたの上司は部下に権力を振りかざす一方で、その上の者（役員など）には服従していますか。					
34	Have your manager shown enough leadership on work? あなたの上司は仕事の上で十分なリーダーシップを発揮していますか。					

Table 27. Questionnaire regarding development of compliance system
Used from Hoshino, et.al (2008, p.163, Table 1.) コンプライアンスシステムの整備

Question Items 質問項目		そう思わない Disagree	あまりそう思わない Tend to disagree	どちらともいえない Neither agree nor disagree	ややそう思う Somewhat agree	そう思う Agree
35	Does a system to check the manager function effectively in your organization? あなたの組織では管理者や経営者をチェックする制度が有効に機能していますか。					
36	Does enough information disclose it at the time of decision making in your workplace? あなたの職場では意思決定に際して十分な情報が開示されますか。					
37	Do you aim to establish a compliance (legal and ethical compliance) in your workplace? あなたの職場ではコンプライアンス（法や倫理の遵守）の確立を目指していますか。					

Table 28. Questionnaire regarding other Single indicators
Used from Hoshino, et.al (2008, p.163, Table 1.) その他の単項目指標

Question Items 質問項目		そう思わない Disagree	あまりそう思わない Tend to disagree	どちらともいえない Neither agree nor disagree	ややそう思う Somewhat agree	そう思う Agree
38	Is the regular employee in your workplace alienated except for special conditions? あなたの職場では、よほどのことがないかぎり正社員が解雇されることはありませんか（雇用保障が高いといえますか）。					

Table 28. (continued).

39	Have your employment regulations been strictly followed in workplace? あなたの職場では就業規則が厳格に守られていますか。					
40	Has the work objective of each person been clear every day? あなたの職場では、各自がその日その日にすべき仕事が明確になっていますか。					
41	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? あなたの組織では、毎年の昇給・昇進の決定に際して前年に各人が達成した業績や成果を直接に反映させていますか。					
42	Is there fierce competition existing in the market activities in your company (organization)? あなたの会社（機関）は市場で激しい競争に直面していますか。					
43	Does your organization produced a good performance and been highly evaluated during the past decade? 過去 10 年ほどの間、あなたの組織は高い業績を挙げていますか。					

APPENDIX (B)

Table 29. The 186 organizational samples where information security incidents (2006-2015)

No	Organization name	Incidents summary
1	Uji city	217,617 of Uji City resident card were leaked
2	TBC	Personally identifiable information leakage incidents
3	Lawson	about 56 million of personally identifiable information of card members was leaked
4	SANYO SHINPAN	Leakage of personally identifiable information
5	Yahoo! BB	Information of 4.62 million people were leaked from Yahoo! BB subscriber list
6	Yahoo! BB	About 560000 personally identifiable information were leaked from Yahoo! BB subscribers name list
7	Japan Net Takata	leakage of customer information
8	ACCA Networks	About 340,000 of customer information were leaked
9	Cosmo Oil Co., Ltd.	Leakage of 92 million of personally identifiable information (Cosmo card member)
10	Nikko	Unauthorized access to Nikko and air ticket booking system
11	PC school	Unauthorized use of student password of PC school
12	E-mail magazine	Leakage of personally identifiable information of customer and e-mail magazine subscribers (400 cases)
13	NTT West "FLET series"	NTT West leakage of "FLET series" contract's e-mail address
14	PC specializes shop	leakage of customer’s email address
15	Sony Sea copy Laboratories	Personally identifiable information of about 1 million people of cosmetics related manufacturers "Sony Sea Pea Laboratories" were leaked
16	Online game	Unauthorized access
17	provider	Unauthorized access
18	Asahi Shimbun	Tampering of Asahi Shimbun website
19	Lawson card	About 280 personally identifiable information were lost.
20	junior high school report card	Information that contain report card has been stolen.
21	woman clinic	Leakage of 280 patients personally identifiable information.
22	Post office member	Unauthorized access to 100000 of customer information.
23	fatherless families	Information of 10 Fatherless family were stolen.
24	Mizuho Bank	Around 5700 Information including (account name, contact, phone, name, address) were lost.
25	AFLAC	About 17,000 personally identifiable information were lost from life insurance company subscriber list of AFLAC
26	Ehime Prefecture	700 of personally identifiable information of has been leaked,
27	Soka city, Saitama	457 of personally identifiable information were leaked.
28	Fire staff of Fujisawa City	information 467 of personally identifiable information were leaked.

Table 29. (continued).

No	Organization name	Incidents summary
29	inmates	12000 of personally identifiable information were leaked
30	Okayama Kurashiki Station	Okayama Kurashiki Station personal PC of the investigation section staff stores the investigation materials, the leakage investigation materials of 1500 people.
31	NHK Hiroshima hosokyoku	Leakage of 150 personally identifiable information (account, name, address, phone)
32	Ehime Prefectural Police	stores the investigation content to PC, information leaked by infection Internet virus (winny)
33	captain	42-year-old captain, leaked password of each airport (winny)
34	TBS saury	About 540 personally identifiable information were leaked.
35	TEPCO	Tokyo Electric Power Company, 23 persons of customer data Society announced, print the 3200 sheets.
36	Meguro Seibigakuen	80 student's name and the score was leaked from the vice-principal by virus(winny)
37	NTT West Japan	unauthorized access.
38	Fukuoka Central Post Office	information that is used for business, personal information of 162 persons was lost.
39	Panasonic Electronic	Information for six employees of the company leaked out from the private possession PC of the employee.
40	Tohoku Labor Banks	Information lost during internal inspection.
41	KDDI IIDA Shopping	Personal information was leaked customer information to another is displayed on the order confirmation screen.
42	JTB Tohoku	An employee transmits an email mistakenly. A file including the personal information was attached for an email.
43	Citi Cards Japan	A contractor acquires a list including the personal information illegally sold to a third party.
44	Hokkaido University	The staff loses USB memory including the secret information
45	Japan Post Group	lost about 32 million of information.
46	Bank of Kyoto	information, including personal information was lost.
47	Ryohin Keikaku	credit card reserve was lost. It turns out when the accountant is trying to process
48	Cecile	the supplier whom Cecile consigned to a past obtains customer information illegally and sells it to a list distributor.
49	Awa Bank, Ltd	microfilm containing information was lost.
50	Keio University Hospital	USB memory that records the information of patients with outpatient visits to Keio University Hospital in whereabouts unknown

Table 29. (continued).

No	Organization name	Incidents summary
51	Miyazaki Taiyo Bank	the CD-ROM in which you saved the transaction record outside the store was lost when the contractor's security company has been replaced.
52	Shiga Bank, Ltd	A journal the ATM which Shiga Bank keeps was lost.
53	Panasonic Hearing Aid Co., Ltd.	The employee lost company cell-phone including the secret information.
54	SAN-IN GODO BANK	USB memory lost contain secret information.
55	TV Asahi	Email mis-sending. E-mail address of 834 cases were leaked.
56	Nature Japan	Unauthorized access
57	Cedyna Financial Corp	The supplier took customer information without permission and sold it.
58	Panasonic Home Elevator	PC including personal information was stolen.
59	Tennis-Gear	Server of Tenisugia is met with unauthorized access
60	GMO Gamepot Inc	On-line games the game pot operated, personal information outflow subject to unauthorized access
61	NTT East Japan	NTT East Japan loses a list including the personal information during a business activity.
62	Kyushu Electric Power Co., Inc.	Contractors of Kyushu Electric Power lost a document that contains personal information.
63	Hanbit Ubiquitous Entertainment	mis-sending email. The delivery to attach an unintended file, e-mail address is outflow.
64	THIRDWAVE CORP	Lost documents that contain personal information.
65	Vento Takanawa shop	Email mis-sending, Personal information were leaked
66	Nagano Bank	carrying out prohibition information outside was lost
67	Anjo Rehabilitation Hospital	PC theft including the personal information of the patient.
68	HOKKAIDO ChuoBus Corp	Personal information was leaked by mis-sending email.
69	Samsung Card	about 800,000 personal information were leaked
70	Mizuho Bank	Documents that contain personal information loss. Determined to be incorrect disposal because the result of the investigation, disposal record is present. Possibility of outflow is low.
71	Yaesu Book Center	Accepted Name list of visitors collected when performing a lecture at Yaesu Book Center was lost.
72	Coop Ehime	lost USB memory containing information of union members
73	Daito Bank, Ltd. Otsuki Branch	the luxurious golden mansion Branch lost information of the customer.
74	Mitsubishi Heavy Industries	Computer virus invasion to internal by employee with employee knows, system information was leaked.
75	Tokai Electronic	information leaked by mis-sending email.
76	GMO Solution Partner	information leakage by the unauthorized access.

Table 29. (continued).

No	Organization name	Incidents summary
77	Tokai Radio Broadcasting Company	leakage of information by mis-sending email.
78	Tokiwa Chemical Industries	leakage of information by mis-sending email.
79	Kurashiki Cable TV	displays 131 email addresses by mis-sending email.
80	Nagano Pref Karuizawa Office	PC containing information about 8617 was lost.
81	Resona Bank	2218 information was lost
82	UPDATE Inc	employee lost his bag which contains secret information
83	GREENPEACE	252 email address leakage by mis-sending email
84	Oita Farm Co-op	USB memory to transfer data of 157 customer information of milk price for November of 2011 was lost
85	NHK	License fee exemption certificate was lost
86	Mitsui Home Co., Ltd.	lost USB memory contains information of the resident of temporary housing of Fukushima.
87	Babycome	login and password e-mail address of the registered members leaked by unauthorized access.
88	Panasonic Associated Companies	invitation was faxed to the 61 shop dealer, the invitation and application form of the workshop of the company held, and in which there is an error in the reply fax number was listed in the invitation.
89	Aflac	files attached were sent containing information such as date of birth and name, address, telephone number, contract information of 2809 reviews payment.
90	Japan Services Organization	attached payment vote mistaken delivered.
91	Nerima Hospital	a doctor has lost USB memory contains information of 45 patients.
92	Vector Inc	information was leaked to the outside by unauthorized access occurs to the server.
93	Yamaha	Name list was lost
94	Daishin	information was leaked by unauthorized access.
95	SUMINOE Co., Ltd.	company mobile phone was lost, about 150 names and telephone numbers have been registered.
96	Nagoya City	Information was stolen from employee car at the parking lot.
97	Sakushin Gakuin University	USB memory was lost.
98	Panahome Corp	Notebook was lost, including customer information.
99	Sagamijoshidai High School	USB memory was lost, name and some test-takers in 2011 from 2008.
100	OsakaTakashimaya co.,ltd.	Lost refrain delivery order form
101	Okinawa Gas	Business mobile phone was lost.
102	Fukuoka Univ Hospital	USB memory was stolen inside car for 68 persons.
103	Baseball Ticket Sales System	ticket sales system has received unauthorized access.
104	Water Server Sales Company.	Purchase application form was lost.

Table 29. (continued).

No	Organization name	Incidents summary
105	Mitsubishi Nagasaki Hospital	lost a USB memory contains 24 patients information
106	Hamamatsu Shinkin	information was lost.
107	Linkedin	Password outflow.
108	Tokyu Hands	name of the 37 people who purchased between May 4 from February 14, 2012, address, phone number, bought and serial number of the gas cylinder has been described.
109	Livesense Inc.	PC contains about 30,000 information of adoption and 27 customer's company, mail data, including personal information of part-time adopters was stolen by theft.
110	Tsuchiura City Library	Email mis-sending
111	Miyazaki Prefecture Resource Recycling Division	Email mis-sending
112	Okinawa Bank	Seal stamp vote was lost.
113	Combi Town	information was leaked by unauthorized access.
114	NET RIDE	SQL injection attack, unauthorized access, information was laked.
115	Saitama Prefecture IT Division	mis-sending email, information about 125 people who are registered in the database.
116	Towa House	information of 76 customers was stolen by theft, unauthorized use of information that has not been confirmed.
117	U.S. Yahoo	Outflow of 450,000 e-mail address and password.
118	Yachiyo Bank	about 1627 information of sign up in 2009 was lost.
119	Osaka University of Economics	IC recorder was lost
120	Osaka City Waterworks Bureau.	Construction application form was lost.
121	Central Tanshi FX Co.,Ltd	mis-sending email
122	Gifu University	2726 surgery data was stolen from car at the parking lot
123	Kagoshima Broadcasting Corporation	Application postcard was lost.
124	Takashimaya Nihonbashi Shop	List of customers was lost.
125	Howa Bank	information lost
126	OKAZAKI SHINKIN BANK	lost of 15,800 information at 8 branch .
127	Sugamo Shinkin Bank	information of customer was lost
128	Nihon Oligo Co.,Ltd	the guide mail about the company's online shop was sent by setting the "CC" e-mail address of the destination, the displayed e-mail address and name of 562.
129	NTT West	Subcontractor employees of NTT West lost information on car parking lot.
130	Sompo Japan	became unknown information’s location in the transportation process.

Table 29. (continued).

No	Organization name	Incidents summary
131	Nerima Shakujii Higashi Elementary School	Teacher lost his bag contain important information.
132	Nagano Prefectural High School	Teacher lost his USB memory which contains information was used in the terminal of the personal computer in the classroom.
133	JP Life Insurance	Lost five note books of employees who had been used in operating activities in Narashino post office
134	Telecom Square,Inc.	Unauthorized access from outside.
135	Ebara Hospital	lost a USB, training physicians put patient information to a USB memory and taking out without permission.
136	CHUNICHI DRAGONS	Unauthorized access from outside.
137	COMTEC	Unauthorized access from outside.
138	Tokyo Metropolitan	information of construction office was lost.
139	Kochi Prefecture	information was lost.
140	Kanazawa Institute of Technology	information was disclosed by teacher who used Google Group.
141	Nirasaki Public elementary school	teacher lost his bag contains information in the car parking lot.
142	Mie University	associate professor lost USB memory contains personal information.
143	Yahoo	The information that began to flow was uploaded on a bulletin board of Tor.
144	Atpages (@pages)	user name and password to access the user management information database to flow out.
145	N.T.Technology	information leaked by the unauthorized access.
146	Kyoto University	information was open through Google Group.
147	Sumitomo Life Insurance	information was disclosed
148	DOWELL Co., Ltd	employee has left mobile phone company in the taxi
149	AMEBA	unauthorized login
150	Waseda University	Google group become accessible state.
151	Jalan Net	unauthorized login from the external
152	GREE	There was a unauthorized login between July 25 to August 5 2013
153	NTT Communications	information was flowed out by the unauthorized access.
154	FUKUHO BANK	information was discarded by mistake
155	LINE	unauthorized access from the outside. Independent company operated or "LINE" and "livedoor" service.
156	NIFTY Corporation	unauthorized login to the company site from outside between 14 to 16, member information is viewed
157	Daito Bunka University	staff taking out the USB memory in order to work at home, the USB was lost.
158	NINTENDO	There was a bad login member site.

Table 29. (continued).

No	Organization name	Incidents summary
159	Tokio Marine & Nichido Life Insurance	Stolen the bag and information for business PC.
160	Daiwa Living	an employee lost information in the car parking lot.
161	Nissen Co., Ltd.	There was a unauthorized login mail order site "Nissen online"
162	TEPCO	employees lost bag contains information on the train in Saitama Prefecture
163	Happinet Online	unauthorized access.
164	Hankyu Hanshin Encyclopedia Shop	There is unauthorized access, membership information is viewed.
165	Chiba Sakura City	Personal information was leaked.
166	XCom Global	SQL injection attack to the server ex-com global operated "GLOBAL DATA" and "Global Cellular", customer information was leaked.
167	ISETAN MITSUKOSHI HOLDINGS	large amount of unauthorized access is performed, it was leaked membership information is viewed.
168	Idemitsu Credit	They update the system, but the prevention measures were not enough, as a result customer information has been viewed on the internet.
169	Bank of Tokyo-Mitsubishi UFJ, Ltd.	Mitsubishi UFJ, Ltd- it is considered that discarded it by mistake after paperwork was over.
170	NTT DoCoMo	NTT DOCOMO USA, Inc. Receives a cyber attack, customer information for Japanese-American MVNO service of "DOCOMO USA Wireless" is leaked.
171	JR East	unauthorized access from a specific IP address.
172	DADWAY INC	information can be viewed state on the site.
173	Fukoku Mutual Life Insurance Company	Fukoku Mutual Life Insurance Company employees lost CD-ROM that contains information.
174	JINS online	information of 12,036 customers who have credit card payment on June 14 to March February 2013was leaked.
175	Akita Bank	employees discarded information by mistake.
176	Suzuki	information can be viewed on the Internet.
177	Benesse	Information of 7.6 million customers were lacked, Subsidiary copied data on recording medium (Smartphone), and sold it externally to a name-list provider
178	Kyushu Electric Power	unauthorized login seen as "password list attack" occurs. The place of the analysis of the access log, attempts number of login amounted to 3,161,872 cases, log in 1320 review account was successful.

Table 29. (continued).

No	Organization name	Incidents summary
179	University of Miyazaki	USB memory that applicant information of faculty recruitment has been saved has become a whereabouts unknown, the name on the applicant of faculty recruitment, address, telephone number, date of birth, etc.
180	Electrical engineers test center	USB memory that contain 578 personally identifiable information was lost.
181	JAL	Some malware is infected with a personal computer, customer information of the JAL Mileage Bank amounting to up to 75 million cases (JMB) in the problem that has been found that there is a possibility that the external flow, the company confirmed the leak of some customer information.
182	Maruhachimawata sales company	The Personally identifiable information of the customer company employee transaction so far revealed that it was sold to third parties.
183	Southern Japanbroadcast	By unauthorized access, about two million personally identifiable information of the members were leaked.
184	Hospital of Fukui University	Laptop contain 11 patients personally identifiable information of has lost.
185	Xijing Shinkin	In Nishi branch, CDRs which records customer information include customer's name, address, telephone number, date of birth, and the 6316 review information such as the account number were lost.
186	Sony's PlayStation Network	the personal information of one hundred million people leaked from its PS3 game console service site because an old software version of Open SSH 4.4 was used, which made it easy for hacker groups to invade it. hacker groups to carry out an SQL injection attack

APPENDIX (C)

Table 30. Correspondence between the company incidents and 11 main factors

	Organization Name	Deterioration of Values	Freewheeling Corporate Culture	Hands-Off Policy	Unclear Objective of the Management	Not Customer-Oriented	Unmanaged Organization	Lack of Sense of Belonging	Organization with Numerous Dissatisfactions	Organization with No Autonomous Control	Organization without Corrections	Organization without Leadership
1	Uji city	1	0	1	0	1	1	1	0	0	0	1
2	TBC	1	0	0	0	1	1	1	1	0	0	1
3	Lawson	0	0	1	0	0	1	1	0	1	0	0
4	SANYO SHINPAN	0	0	0	1	1	0	1	0	1	0	0
5	Yahoo! BB	1	1	1	0	1	1	1	0	1	0	1
6	Yahoo! BB	1	0	1	0	0	1	1	0	1	0	1
7	Japan Net Takata	1	0	1	0	0	1	1	0	0	0	0
8	ACCA Networks	1	0	1	0	1	1	1	0	0	0	0
9	Cosmo Oil Co., Ltd.	1	0	0	0	1	1	1	0	0	0	0
10	Nikko	1	0	1	0	1	1	1	0	0	0	0
11	PC school	1	0	1	0	1	1	1	0	0	0	0
12	E-mail magazine	0	1	1	0	1	1	0	0	0	0	0
13	NTT West "FLET series"	1	0	1	0	0	1	1	0	0	0	0
14	PC specializes shop	1	0	1	0	1	1	1	0	0	0	0
15	Sony Sea copy Laboratories	1	0	1	0	0	1	1	0	0	0	0
16	Online game	0	1	1	0	0	1	0	0	0	1	0
17	provider	1	0	0	0	0	1	0	1	1	1	0
18	Asahi Shimbun	1	0	1	0	1	0	1	0	0	0	1
19	Lawson card	1	0	1	0	0	1	1	0	0	0	1
20	junior high school report card	1	1	0	1	1	1	0	1	1	0	1
21	woman clinic	1	0	0	1	0	1	0	0	1	1	1
22	Post office member	1	1	0	1	1	1	0	1	1	0	0

Table 30. (continued).

	Organization Name	Deterioration of Values	Freewheeling Corporate Culture	Hands-Off Policy	Unclear Objective of the Management	Not Customer-Oriented	Unmanaged Organization	Lack of Sense of Belonging	Organization with Numerous Dissatisfactions	Organization with No Autonomous Control	Organization without Corrections	Organization without Leadership
23	fatherless families	1	0	0	0	1	0	0	1	1	0	0
24	Mizuho Bank	1	0	1	0	1	0	0	0	1	0	0
25	AFLAC	1	0	1	1	1	0	0	0	1	0	0
26	Ehime Prefecture	1	0	0	0	1	1	0	0	1	0	0
27	Soka city, Saitama	1	1	1	0	1	0	0	1	1	0	0
28	Fire staff of Fujisawa City	1	0	1	1	1	1	0	0	1	0	0
29	inmates	1	0	1	0	1	1	0	0	1	0	0
30	Okayama Kurashiki Station	1	1	1	0	1	1	0	0	1	0	0
31	NHK Hiroshima hosokyoku	0	1	1	1	0	1	0	0	0	0	1
32	Ehime Prefectural Police	1	1	1	0	1	0	0	0	1	0	0
33	captain	1	1	1	0	1	1	0	0	1	1	1
34	TBS saury	1	1	1	0	1	1	0	0	1	0	1
35	TEPCO	1	1	1	0	1	1	0	0	1	0	0
36	Meguro Seibigakuen	1	1	1	0	1	1	0	0	1	0	0
37	NTT West Japan	1	1	0	1	1	1	1	1	1	0	1
38	Fukuoka Central Post Office	1	1	1	1	1	1	0	1	1	1	1
39	Panasonic Electronic	0	0	0	1	1	1	0	0	0	0	0
40	Tohoku Labor Banks	0	0	1	1	0	1	0	0	0	0	0
41	KDDI IIDA Shopping	1	0	0	0	0	0	1	1	0	1	0
42	JTB Tohoku	1	1	1	0	0	1	0	0	1	0	1
43	Citi Cards Japan	0	0	1	0	0	1	1	0	0	0	0
44	Hokkaido University	1	1	1	0	1	1	0	0	1	0	1
45	Japan Post Group	1	1	1	0	1	1	0	0	1	1	1
46	Bank of Kyoto	0	0	0	1	0	0	0	0	0	0	0
47	Ryohin Keikaku	0	0	0	0	1	0	1	0	0	0	0
48	Cecile	0	0	1	1	1	1	0	0	0	0	0

Table 30. (continued).

	Organization Name	Deterioration of Values	Freewheeling Corporate Culture	Hands-Off Policy	Unclear Objective of the Management	Not Customer-Oriented	Unmanaged Organization	Lack of Sense of Belonging	Organization with Numerous Dissatisfactions	Organization with No Autonomous Control	Organization without Corrections	Organization without Leadership
49	Awa Bank, Ltd	0	0	0	1	0	1	0	0	0	0	0
50	Keio University Hospital	1	1	0	1	0	0	0	1	0	0	1
51	Miyazaki Taiyo Bank	1	0	1	0	0	1	1	0	1	0	0
52	Shiga Bank, Ltd	0	0	0	1	0	1	0	0	0	0	0
53	Panasonic Hearing Aid Co., Ltd.	0	0	0	0	1	1	0	0	0	0	0
54	SAN-IN GODO BANK	1	0	0	1	0	0	1	0	0	1	0
55	TV Asahi	1	1	0	1	1	1	0	0	1	0	1
56	Nature Japan	0	0	0	0	1	1	0	0	1	0	1
57	Cedyna Financial Corp	1	1	0	0	1	1	1	0	0	1	0
58	Panasonic Home Elevator	0	0	0	0	1	1	0	0	0	0	0
59	Tennis-Gear	0	1	0	0	1	0	0	1	1	0	1
60	GMO Gamepot Inc	0	1	0	1	1	1	0	1	0	0	0
61	NTT East Japan	1	1	1	0	0	0	1	1	0	0	1
62	Kyushu Electric Power Co., Inc.	1	0	0	1	0	0	1	1	0	1	0
63	Hanbit Ubiquitous Entertainment	1	1	0	0	0	1	0	0	1	0	0
64	THIRDWAVE CORP	0	1	1	0	1	0	0	1	0	1	1
65	Vento Takanawa shop	1	1	0	1	1	0	0	1	1	0	1
66	Nagano Bank	1	1	0	0	0	1	0	0	1	0	1
67	Anjo Rehabilitation Hospital	0	1	0	1	1	0	0	1	1	0	1
68	HOKKAIDO ChuoBus Corp	1	1	0	0	1	1	0	1	0	1	0
69	Samsung Card	1	1	1	0	0	1	0	0	1	0	1
70	Mizuho Bank	0	0	0	0	1	1	0	0	1	0	0
71	Yaesu Book Center	0	1	1	0	0	1	0	0	0	1	1

Table 30. (continued).

	Organization Name	Deterioration of Values	Freewheeling Corporate Culture	Hands-Off Policy	Unclear Objective of the Management	Not Customer-Oriented	Unmanaged Organization	Lack of Sense of Belonging	Organization with Numerous Dissatisfactions	Organization with No Autonomous Control	Organization without Corrections	Organization without Leadership
72	Coop Ehime	0	0	1	0	1	1	0	0	0	0	1
73	Daito Bank, Ltd. Otsuki Branch	1	1	0	1	0	1	0	0	0	1	1
74	Mitsubishi Heavy Industries	0	0	1	0	0	1	0	1	0	1	1
75	Tokai Electronic	0	0	1	0	0	1	0	0	1	0	0
76	GMO Solution Partner	0	0	0	1	1	1	0	0	1	0	0
77	Tokai Radio Broadcasting	1	0	0	0	1	0	1	0	0	1	0
78	Tokiwa Chemical Industries	1	1	0	0	0	1	0	0	1	0	0
79	Kurashiki Cable TV	1	1	0	1	0	0	0	0	0	0	0
80	Nagano Prefecture Karuizawa Office	1	0	0	0	0	1	0	0	0	0	0
81	Resona Bank	1	1	1	0	0	1	0	0	0	0	1
82	UPDATE Inc	1	0	0	0	0	1	1	0	0	0	0
83	GREENPEACE	1	0	0	0	0	0	0	0	1	0	0
84	Oita Farm Co-op	0	1	0	0	0	0	0	1	1	0	0
85	NHK	0	0	0	0	0	1	1	0	1	0	0
86	Mitsui Home Co., Ltd.	0	0	0	0	1	1	1	0	1	1	0
87	Babycome	1	1	0	0	0	0	0	0	0	0	1
88	Panasonic Associated Companies	0	0	0	1	0	0	0	0	1	0	1
89	Aflac	0	1	0	1	0	1	1	1	1	1	1
90	Japan Services Organization	0	0	0	0	0	0	0	0	0	0	0
91	Nerima Hospital	1	1	0	0	0	1	0	0	1	0	1
92	Vector Inc	1	0	1	0	1	0	1	1	1	1	0
93	Yamaha	0	0	0	0	0	0	0	1	1	1	1
94	Daishin	0	1	0	0	0	0	0	0	0	1	1
95	SUMINOE Co., Ltd.	1	1	1	1	1	0	0	0	0	0	0

Table 30. (continued).

	Organization Name	Deterioration of Values	Freewheeling Corporate Culture	Hands-Off Policy	Unclear Objective of the Management	Not Customer-Oriented	Unmanaged Organization	Lack of Sense of Belonging	Organization with Numerous Dissatisfactions	Organization with No Autonomous Control	Organization without Corrections	Organization without Leadership
96	Nagoya City	0	0	0	1	0	1	0	1	1	1	0
97	Sakushin Gakuin University	1	1	1	1	0	0	1	1	1	1	0
98	Panahome Corp	1	0	1	1	0	0	0	0	0	0	1
99	Sagamijoshidai High School	1	1	1	0	0	1	1	0	0	0	0
100	OsakaTakashimaya co.,ltd.	0	0	1	1	0	0	0	0	0	1	1
101	Okinawa Gas	1	0	1	0	0	1	1	0	1	1	0
102	Fukuoka Univ Hospital	0	0	1	1	0	0	0	0	1	1	1
103	Baseball Ticket Sales System	0	0	0	0	0	1	1	0	1	0	0
104	Water Server Sales Co.	1	1	0	1	1	0	0	0	0	0	1
105	Mitsubishi Nagasaki Hospital	0	0	0	0	1	1	1	1	0	0	1
106	Hamamatsu Shinkin	1	1	1	0	0	0	1	0	1	1	0
107	Linkedin	0	0	0	1	1	1	0	1	0	0	1
108	Tokyu Hands	1	1	0	0	1	1	0	0	1	1	0
109	Livesense Inc.	1	1	0	0	0	0	1	1	0	1	0
110	Tsuchiura City Library	0	0	0	0	0	1	1	0	0	0	1
111	Miyazaki Prefecture Resource Recycling Division	1	1	0	1	0	1	1	0	1	1	1
112	Okinawa Bank	0	1	1	0	1	0	0	1	0	1	0
113	Combi Town	1	0	0	1	1	1	0	0	0	0	1
114	NET RIDE	1	0	1	1	0	0	1	1	1	0	1
115	Saitama Prefecture IT Div.	0	1	1	0	0	1	0	1	0	1	1
116	Towa House	0	0	0	0	1	1	1	0	1	0	0
117	U.S. Yahoo	1	0	1	0	1	0	0	1	0	0	1
118	Yachiyo Bank	1	1	0	0	1	1	0	0	1	1	1
119	Osaka University of Economics	1	1	0	1	0	1	1	0	0	1	0

Table 30. (continued).

	Organization Name	Deterioration of Values	Freewheeling Corporate Culture	Hands-Off Policy	Unclear Objective of the Management	Not Customer-Oriented	Unmanaged Organization	Lack of Sense of Belonging	Organization with Numerous Dissatisfactions	Organization with No Autonomous Control	Organization without Corrections	Organization without Leadership
120	Osaka City Waterworks Bureau.	0	0	1	0	1	0	0	0	0	1	1
121	Central Tanshi FX Co.,Ltd	0	0	0	0	0	1	1	0	1	0	0
122	Gifu University	0	1	0	1	1	1	0	0	1	1	0
123	Kagoshima Broadcast Corp	1	1	1	0	0	0	0	0	0	0	1
124	Takashimaya Nihonbashi Shop	0	0	1	0	1	1	1	0	1	0	1
125	Howa Bank	1	1	1	1	1	0	0	0	0	0	0
126	OKAZAKI SHINKIN BANK	1	1	0	1	0	1	1	1	0	1	0
127	Sugamo Shinkin Bank	0	0	1	0	0	0	0	1	0	0	0
128	Nihon Oligo Co.,Ltd	1	1	0	1	1	1	0	0	1	1	0
129	NTT West	1	0	0	0	0	1	1	1	0	1	0
130	Sompo Japan	0	1	0	0	1	1	0	1	0	0	0
131	Nerima Shakujii Higashi Elementary School	1	1	0	1	0	1	0	1	0	0	1
132	Nagano Prefectural High School	1	1	0	1	0	1	0	1	0	0	1
133	JP Life Insurance	0	0	1	0	1	0	1	0	1	1	0
134	Telecom Square,Inc.	1	1	1	0	0	0	0	0	0	0	1
135	Ebara Hospital	1	0	0	1	0	0	1	0	0	1	1
136	CHUNICHI DRAGONS	0	1	0	0	0	1	0	0	1	0	1
137	COMTEC	0	0	0	0	1	1	0	1	0	0	1
138	Tokyo Metropolitan	0	0	1	0	1	0	0	0	1	1	0
139	Kochi Prefecture	1	1	0	0	0	0	1	1	0	1	0
140	Kanazawa Institute of Tech	1	0	0	0	1	1	0	1	0	1	0
141	Nirasaki Public elementary school	0	1	0	0	0	1	0	0	0	1	1

Table 30. (continued).

	Organization Name	Deterioration of Values	Freewheeling Corporate Culture	Hands-Off Policy	Unclear Objective of the Management	Not Customer-Oriented	Unmanaged Organization	Lack of Sense of Belonging	Organization with Numerous Dissatisfactions	Organization with No Autonomous Control	Organization without Corrections	Organization without Leadership
142	Mie University	1	1	0	0	0	0	1	1	0	0	0
143	Yahoo	0	0	0	0	0	1	1	0	0	0	1
144	Atpages (@pages)	0	1	1	0	0	0	0	0	0	1	1
145	N.T.Technology	1	0	1	1	1	1	0	0	0	0	0
146	Kyoto University	1	1	0	0	0	0	0	1	1	1	1
147	Sumitomo Life Insurance	0	1	0	0	0	0	1	0	0	0	0
148	DOWELL Co., Ltd	1	0	1	1	1	0	0	0	0	0	0
149	AMEBA	0	0	0	0	0	1	1	0	1	0	0
150	Waseda University	1	0	0	0	0	1	1	1	0	0	0
151	Jalan Net	0	1	0	0	0	0	0	0	1	0	1
152	GREE	1	1	1	0	0	0	0	0	0	1	1
153	NTT Communications	0	0	0	0	0	1	1	1	0	0	0
154	FUKUHO BANK	1	1	0	0	0	1	0	0	0	0	1
155	LINE	1	1	1	0	0	0	0	0	0	0	0
156	NIFTY Corporation	0	0	0	0	0	1	1	0	1	0	0
157	Daito Bunka University	0	0	0	0	0	1	1	0	1	0	0
158	NINTENDO	0	0	0	0	1	1	1	0	0	0	1
159	Tokio Marine & Nichido Life	0	1	0	1	1	0	0	0	0	1	1
160	Daiwa Living	0	1	0	0	0	0	1	1	1	0	0
161	Nissen Co., Ltd.	0	0	0	1	0	0	0	0	0	0	0
162	TEPCO	1	0	0	0	0	1	1	1	0	1	0
163	Happinet Online	0	1	1	1	0	0	0	0	0	0	0
164	Hankyu Hanshin Encyclopedia Shop	0	0	0	0	0	0	0	1	1	1	1
165	Chiba Sakura City	0	0	0	1	0	0	0	0	0	0	0
166	XCom Global	0	1	0	0	0	0	1	0	0	0	0

Table 30. (continued).

	Organization Name	Deterioration of Values	Freewheeling Corporate Culture	Hands-Off Policy	Unclear Objective of the Management	Not Customer-Oriented	Unmanaged Organization	Lack of Sense of Belonging	Organization with Numerous Dissatisfactions	Organization with No Autonomous Control	Organization without Corrections	Organization without Leadership
167	ISETAN MITSUKOSHI HOLDINGS	0	1	0	1	1	0	0	0	0	0	0
168	Idemitsu Credit	0	1	0	0	0	0	0	0	1	0	0
169	Bank of Tokyo-Mitsubishi UFJ, Ltd.	0	1	0	0	0	1	0	0	0	0	0
170	NTT DoCoMo	0	1	1	0	0	0	0	0	1	0	0
171	JR East	0	0	0	1	0	0	0	1	0	0	0
172	DADWAY INC	0	1	1	1	1	1	0	0	0	0	0
173	Fukoku Mutual Life Insurance Company	1	0	0	1	1	1	0	0	1	0	0
174	JINS online	1	0	0	0	0	1	0	0	0	1	0
175	Akita Bank	0	0	0	0	0	1	0	0	1	1	1
176	Suzuki	1	1	0	0	1	1	0	1	0	0	0
177	Benesse	1	0	0	0	1	1	0	0	0	1	0
178	Kyushu Electric Power	0	1	0	0	0	1	0	0	0	1	0
179	University of Miyazaki	1	0	1	0	0	1	0	0	0	1	0
180	Electrical engineers test center	1	1	0	0	0	1	0	0	1	0	0
181	JAL	1	0	0	0	0	1	0	0	1	0	1
182	Maruhachimawata sales company	1	1	1	0	1	1	0	0	0	1	1
183	Southern Japanbroadcast	0	0	1	0	0	1	0	0	1	0	0
184	Hospital of Fukui University	1	0	1	0	0	1	0	0	0	1	0
185	Xijing Shinkin	1	0	0	1	0	1	0	0	0	1	0
186	Sony's PlayStation Network	1	0	0	1	0	0	0	0	1	1	0

APPENDIX (D):

Table 31. Sample score for Three factors

Sample No	First factor	Second factor	Third factor
s1	-0.958	-0.645	-0.01
s2	-0.649	0.712	0.758
s3	-1.845	-0.887	0.393
s4	0.067	-1.169	2.146
s5	-0.666	-0.485	-0.485
s6	-1.103	-0.409	-0.239
s7	-1.751	-0.621	0.569
s8	-1.393	-1.007	0.55
s9	-1.54	-0.684	1.309
s10	-1.393	-1.007	0.55
s11	-1.393	-1.007	0.55
s12	-0.199	-1.277	-1.055
s13	-1.751	-0.621	0.569
s14	-1.393	-1.007	0.55
s15	-1.751	-0.621	0.569
s16	-0.069	0.282	-1.305
s17	-0.191	1.388	0.242
s18	-0.893	-0.497	-0.155
s19	-1.158	-0.264	-0.106
s20	0.814	0.091	0.156
s21	0.787	0	0.174
s22	0.756	-0.062	0.579
s23	-0.048	0.522	0.373
s24	-0.512	-1.514	-0.779
s25	0.694	-1.664	0.33
s26	-0.632	-1.285	0.022
s27	0.043	0.152	-0.652
s28	0.364	-1.617	0.395
s29	-0.666	-1.488	-0.48
s30	-0.346	-1.052	-0.887
s31	1.179	-0.731	-0.546
s32	-0.159	-0.986	-1.207
s33	-0.038	-0.183	-1.082
s34	-0.123	-0.736	-1.161
s35	-0.346	-1.052	-0.887
s36	-0.346	-1.052	-0.887
s37	0.228	0.222	0.61
s38	0.626	0.212	-0.177
s40	1.143	-1.983	0.999

Table 31. (continued).

Sample No	First factor	Second factor	Third factor
s41	-0.826	2.682	1.411
s42	-0.151	-0.433	-1.434
s43	-2.183	-0.804	0.825
s44	-0.123	-0.736	-1.161
s45	-0.038	-0.183	-1.082
s46	5.517	-2.264	4.768
s47	-2.211	-0.64	2.359
s48	0.867	-2.124	0.867
s50	1.717	1.159	0.193
s51	-1.566	-0.724	0.275
s53	-0.623	-1.966	0.594
s54	0.29	0.655	2.072
s55	0.779	-0.73	-0.125
s56	-0.215	-0.975	-0.631
s57	-0.725	0.346	0.298
s58	-0.623	-1.966	0.594
s59	0.546	0.89	-0.808
s60	1.316	0.154	1.032
s61	-0.366	1.172	-0.341
s63	-0.329	-0.366	-0.827
s64	0.553	1.162	-1.025
s65	1.113	0.302	0.076
s66	-0.02	-0.06	-1.223
s67	1.375	0.364	0.122
s68	0.194	1.109	-0.056
s69	-0.151	-0.433	-1.434
s70	-0.692	-1.689	0.094
s71	0.188	0.459	-1.605
s72	-0.209	-1.267	-1.027
s73	1.134	0.376	-0.162
s74	0.147	1.403	-0.597
s75	-0.973	-1.606	-0.892
s76	0.861	-1.833	1.263
s77	-1.079	0.584	0.999
s78	-0.329	-0.366	-0.827
s79	2.106	-0.404	0.55
s80	-0.869	-0.727	0.259
s81	-0.015	-0.293	-1.54

Table 31. (continued).

Sample No	First factor	Second factor	Third factor
s82	-2.067	-0.062	1.588
s83	-0.642	-0.603	-0.551
s84	0.492	1.945	-0.567
s85	-2.192	-0.415	1.352
s86	-1.195	-0.022	0.801
s87	0.671	0.739	-1.976
s88	1.967	-0.745	0.352
s89	0.378	1.039	0.586
s90	0.147	1.403	-0.597
s91	-0.02	-0.06	-1.223
s92	-0.7	0.678	0.389
s93	0.499	2.39	-0.529
s94	1.009	1.992	-2.085
s95	1.111	-1.212	-0.073
s96	1.003	0.95	1.235
s97	0.229	0.769	0.513
s98	1.368	-0.868	-0.181
s99	-1.15	-0.272	-0.129
s100	1.622	0.072	-0.264
s101	-1.212	0.011	0.141
s102	1.131	-0.169	-0.392
s103	-2.192	-0.415	1.352
s104	1.514	-0.519	-0.137
s105	-0.688	0.869	0.95
s106	-0.789	0.429	-0.465
s107	1.308	0.163	1.054
s108	-0.119	-0.054	-0.56
s109	-0.41	2.371	0.545
s110	-1.511	0.351	0.718
s111	0.189	0.299	0.296
s112	0.42	1.161	-0.668
s113	1.006	-1.021	0.59
s114	0.177	0.358	0.677
s115	0.332	1.356	-0.984
s116	-1.634	-0.949	1.132
s117	0.21	0.417	-0.579
s118	0.071	0.12	-0.881

Table 31. (continued).

Sample No	First factor	Second factor	Third factor
s119	0.188	0.394	1.014
s120	0.252	0.001	-1.337
s121	-2.192	-0.415	1.352
s122	0.876	-0.42	0.267
s123	0.303	-0.021	-2.103
s124	-1.021	-0.822	-0.128
s125	1.111	-1.212	-0.073
s126	0.312	1.172	1.173
s127	0.125	1.772	-0.182
s128	0.686	-0.37	0.201
s129	-0.918	1.869	1.272
s130	0.265	0.759	0.098
s131	1.216	0.736	0.28
s132	1.216	0.736	0.28
s133	-1.099	-0.205	0.16
s134	0.303	-0.021	-2.103
s135	0.475	0.757	1.096
s136	0.088	-0.057	-1.48
s137	0.255	0.769	0.125
s138	-0.259	-0.574	-0.861
s139	-0.41	2.371	0.545
s140	-0.018	1.105	0.517
s141	0.435	1.149	-1.385
s142	-0.652	2.042	0.813
s143	-1.511	0.351	0.718
s144	0.556	0.919	-2.186
s145	0.603	-1.714	0.654
s146	0.466	1.769	-0.873
s147	-1.604	1.198	0.663
s148	1.075	-1.797	0.639
s149	-2.192	-0.415	1.352
s150	-1.287	1.415	1.722
s151	0.546	0.385	-2.211
s152	0.354	0.721	-1.788
s153	-1.564	1.911	2.362
s154	0.182	0.209	-1.303
s155	-0.001	-0.416	-1.868
s156	-2.192	-0.415	1.352

Table 31. (continued).

Sample No	First factor	Second factor	Third factor
s157	-2.192	-0.415	1.352
s158	-1.123	-0.374	0.656
s159	1.717	0.233	-0.203
s160	-0.746	1.776	0.636
s161	5.517	-2.264	4.768
s162	-0.918	1.869	1.272
s163	1.989	-1.147	-0.213
s164	0.499	2.39	-0.529
s165	5.517	-2.264	4.768
s166	-1.604	1.198	0.663
s167	2.27	-1.23	0.773
s168	0.212	-0.005	-1.913
s169	-0.015	-0.129	-1.103
s170	-0.126	-0.77	-2.104
s171	3.285	1.79	3.445
s172	0.945	-1.474	0.11
s173	0.598	-1.481	0.971
s174	-0.393	0.744	-0.003
s175	-0.086	0.584	-0.881
s176	0.122	0.593	0.039
s177	-0.285	-0.079	0.116
s178	0.176	1.143	-0.911
s179	-0.496	-0.017	-0.624
s180	-0.329	-0.366	-0.827
s181	-0.339	-0.356	-0.799
s182	0.075	-0.047	-1.107
s183	-0.973	-1.606	-0.892
s184	-0.496	-0.017	-0.624
s185	1.084	-0.008	1.19
s186	1.198	0.054	0.785