IIPS

Institute for
International Policy Studies

•

IIPS Policy Paper 269E
March 2001

Corporate risk and information security

Akio Kunii

INSTITUTE FOR INTERNATIONAL POLICY STUDIES

The Institute for International Policy Studies was established in June 1988 as an independent research center. In cooperation with other domestic and international research organizations, IIPS examines global security, economic, and environmental issues, and proposes policies to address present and future trends. The Institute issues papers in Japanese and English, publishes a quarterly newsletter, and produces *Asia-Pacific Review,* a journal of debate on the Asia-Pacific region.

INSTITUTE FOR INTERNATIONAL POLICY STUDIES,
Toranomon 5 Mori Building, 5F,
1-17-1 Toranomon, Minato-ku, Tokyo 105-0001, Japan

Telephone: (03) 5253-2511
Facsimile: (03) 5253-2510

IIPS POLICY PAPERS are written by distinguished research fellows, senior research fellows, and visiting scholars of the Institute for International Policy Studies. The views expressed in each paper are those of the author and do not necessarily represent the views of the Institute for International Policy Studies.

For additional copies, reprints and permissions, or other information, please contact:

IIPS PUBLICATIONS DEPARTMENT
Toranomon 5 Mori Building, 5F,
1-17-1 Toranomon, Minato-ku, Tokyo 105-0001, Japan

Telephone: (03) 5253-2511
Facsimile: (03) 5253-2510
E-mail: editor@iips.org

Corporate Risk and Information Society

AKIO KUNII

In the past, as far as most companies were concerned, information security had meant protection of hardware. With rapid advancement in technology, however, and the increasing importance of information systems to companies, new and ever more sophisticated dangers have begun to emerge. Based on a survey of major Japanese companies, IIPS Senior Research Fellow Akio Kunii examines the extent to which corporations are affected by these new threats, such as illegal cyber hackers, and the lessons to be learnt when formulating countermeasures. Focusing on four priorities—employee efficiency, convenience of customer and dealer, security and cost—Kunii analyzes industry trends and the implications of the manner in which a company had introduced IT. The results revealed the significance of an effective chief information officer. Kunii concludes that to succumb to the charms of IT in haste, may lead to repent in leisure, as it is self-evident that decisions not based on a clear and carefully coordinated plan may bring about unwarranted results.

According to a 1998 report by the Japan Society of Security Management, "[In the past,] security measures on the spread of information technology (IT) (*johoka*) [had] tended to focus on protecting computer hardware from physical damage such as that from fire and natural disasters by placing them in secure buildings that were fully equipped with emergency equipment." [1] With the spread of IT and proliferation of computer networks, however, information systems have become ever more important to companies, and this, in turn, has brought a new breed of risk to light.

In addition to past threats to corporate information systems, such as a break down or crash (as exemplified by the Y2K problem in the year 2000), and direct attacks, such as hacking into the corporate network, sending cyber viruses and leaking customer details, hitherto unprecedented hazards have also arisen. These include the illegal acquisition of Internet domain names—cyber squatting—and disputes with individual consumers who are able to exploit the Internet's potential, as was the case in the 1999 "Toshiba Incident."[2] Companies have had to place more weight on the security of their information systems.

According to Toshiaki Otsuka, "Information security management by companies can be divided into the following three areas...management security, system security and hardware security." Security measures to "protect against physical damage such as from disasters," as was mentioned at the beginning of this article, would come under "hardware security." On the other hand, in more recent times "system security" and "management security" have become more important.[3]

This article will examine the current situation of the risks in these three areas, and analyse the structural factors behind the risks companies take when making decisions, based on a survey of major Japanese companies.

Current situation of IT security

System security

In February 2001, the web pages of almost 100 Japanese companies were broken into by a Chinese hacker group called the Honker Union of China (HUC).[4] This type of illegal cyber hacking has almost become a daily occurrence. According to Yasui, around 35 percent of companies in Japan have fallen prey to cyber hackers via the Internet, and around 80 percent of them have been affected by computer viruses.[5] Many high-profile Japanese companies and organizations have been targets of attacks on their web pages. Notably, in June 1999, the home pages of two major media companies, *Asahi Shimbun* and *Mainichi Shimbun*, were attacked in what was essentially the first recognized case of this kind of cyber attack against a major Japanese company. This was followed soon after by attacks on several Japanese government web pages in the week from 24 to 31 January 2000.[6]

In March of the same year, the websites of Kyushu Bank and Kobe Shinyo Kinko (Bank) were attacked. With e-commerce set to expand, these incidents have given rise to concerns about the security of information systems of financial institutions that constitute the infrastructure of e-commerce. For example, from 7 to 9 February 2000, Distributed Denial of Service (DDoS) attacks by computer hackers crashed the servers of several prominent American commercial websites such as Yahoo!, eBay, CNN, amazon.com, and E*TRADE. These attacks were a disaster for commerce.[7]

Illegal access to information systems, which can now be considered the infrastructure for socioeconomic activity, has become so common that organizations that use information systems are being forced to be extremely vigilant towards the security of their systems.

Management security

Management security has also become more important. In 1999, huge quantities of customer details were leaked from Nippon Telephone and Telegraph East Corporation (NTT East). Since then, there has been a spate of similar incidents at several companies, including other telecoms such as J-Phone and KDDI, temporary staff agencies and life insurance companies. Neither is the problem confined to the private sector, as an entire register with residents' details was leaked from the computers of a local government in Kyoto Prefecture. Information systems have made it easier for confidential information such as customer details to be leaked in this way, and the number of incidents has become too frequent to enumerate.

Companies have adopted various countermeasures, such as sealing up the floppy disk drives of computer terminals and censoring email messages to, and from, their employees. However, many of these measures may be overly dependent on the actual systems themselves. Meanwhile, with only about 23 percent of Japanese companies establishing formal security policies, they have been much slower to implement managerial measures, such as employee education and clarification of policy.[8]

The range of domain names available to Japanese organizations has increased, with not only ccTLD (country domain) names such as "co.jp," but also gTLD (generic domain) names such as ".com," ".org" and ".net," Japanese language domains, and ".jp" (universal jp domains) becoming options. Under these circumstances, many of the major companies in Japan today are spending considerable amount of resources and energy on countermeasures against

cyber-squatting. To protect their company name, trademarks and brands, they are using large numbers of human resources, instigating legal actions such as lawsuits and arbitration, and other measures. As a case in point, Hitachi Ltd. has registered and transferred around 150 domain names in 120 countries around the world.[9] For these companies, cyber-squatting is an area in which the burdens of devising and implementing risk countermeasures are enormous.

Current status of information security management in Japanese companies

Overview of survey

In light of this, a survey of the major Japanese companies was taken to clarify the structure of risk occurrence in these companies.

In February 2001, questionnaires were posted out to the managers of the management planning and information systems divisions of 2000 Japanese companies.[10] These companies were selected by random sampling from listed companies and major life insurance companies in Japan. Responses were received from 186 companies, for a valid response rate of 9.3 percent.[11]

The main points of the survey included "cyber hacking of information systems," "leaks and control of important information," and "decision-making on information systems."

Characteristics of companies surveyed

Demographics

Most of the companies surveyed were listed companies and the rest were major life insurance companies, and as such, they represented some of Japan's largest enterprises.

The average profile of a survey respondent was "a company with several thousand employees, several dozen places of business in Japan and several places of business overseas." As can be seen in figure 1, based on industry, manufacturers accounted for more than half of the respondents, and the remainder included service, construction, commerce and financial institutions.

Introduction of IT

The results of the survey in figure 1 show that the proliferation of IT really took off from 1995 onwards, with high scoring responses for "established corporate website" (94 percent of the respondents as of 2001), "email" (89 percent), "use of Internet browsers" (87 percent), and "groupware" (84 percent).

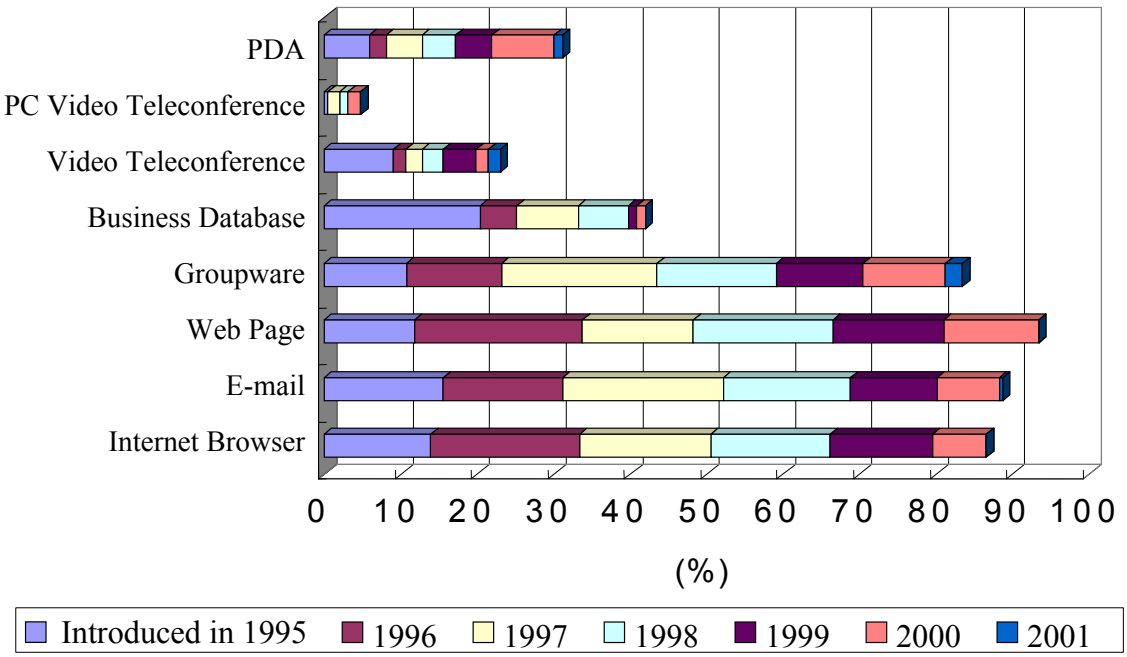


Figure 1 Status of IT Introduction

Figure 1 also clearly shows that, back in 1995, most of the respondents had not introduced IT on a company-wide scale, with the exception of the 20 percent or so of companies that had introduced "data bases." By 1996, around one-third had introduced Internet-related IT such as "email" and "use of Internet browsers," and this number jumped rapidly to around two-thirds in the following three years to 1998.

The patterns of introducing IT were analysed using quantification method of type III using 0-1 dummy variables. This analysis revealed that patterns in introducing IT could be explained by the following three broad components: component 1, which indicates the quantitative aspects of introducing IT; component 2, which shows whether or not the IT introduced is Internet-related; and component 3, which describes the scale of IT systems introduced.

By plotting the status of introducing IT of the 186 respondents for the seven years from 1995 to 2001 calculated onto a two-dimensional space, the relationship between components 1 and 2, for example, can be illustrated as in figure 2. In this case, the further to the right of the graph a company's position, the greater the level of IT it has introduced (a greater variety of IT has been introduced).

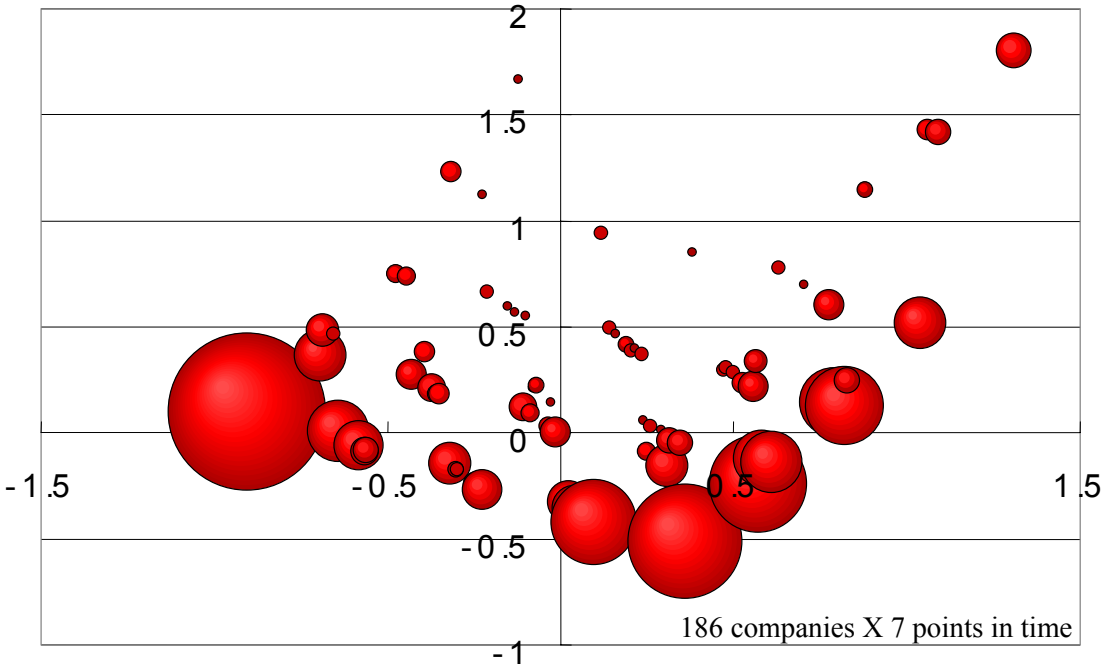


Figure 2 Status of IT introduction (components 1 and 2)

Companies distributed towards the bottom of the graph show a tendency to lean more towards Internet-related IT, whereas companies in the upper half show a more balanced pattern of IT introduction. The size of the circles in indicates the number of companies with the same component score in the same year, or, in other words, the same level of IT introduction.

As the IT introduction patterns of the 186 respondents at seven points in time (1995–2001) are shown in one graph, there should be 186 × 7 = 1302 points plotted on the graph. Companies with exactly the same pattern are plotted on the same point in the two-dimensional space, so larger circles are used to indicate the number of companies with the same pattern.

The following figures are distribution graphs of the status of IT introduction (component 1 x component 2) between 1995 and 2001, with the results for 1995 (figure 3), 1998 (figure 4), and 2001 (figure 5) being used as examples.

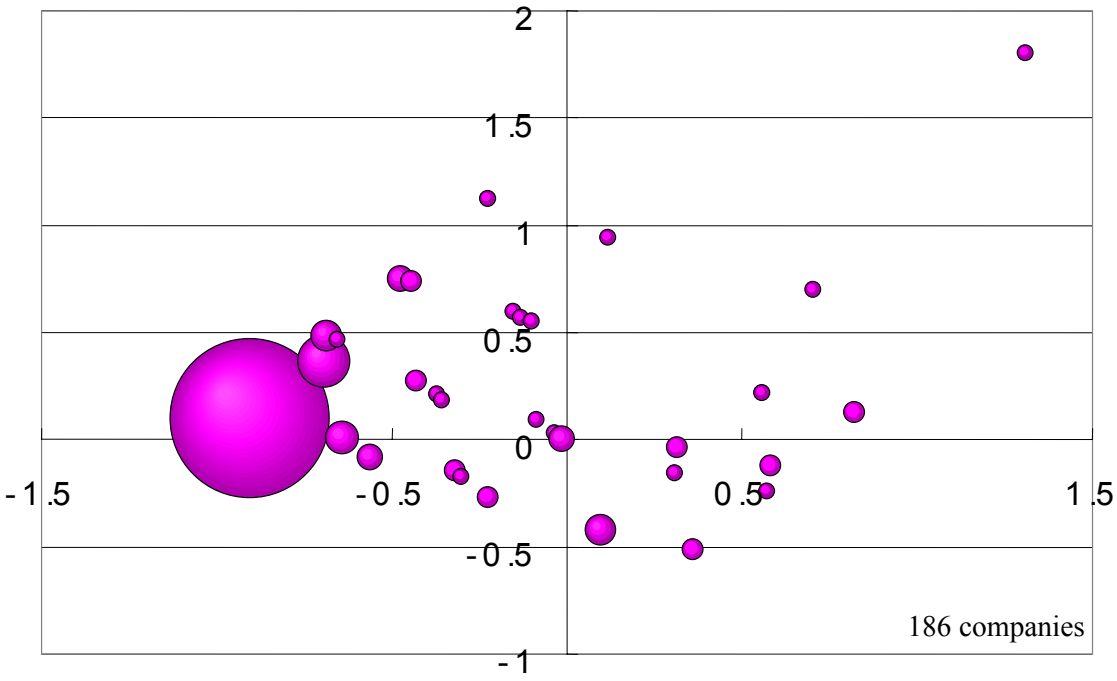


Figure 3 Status of IT proliferation in 1995

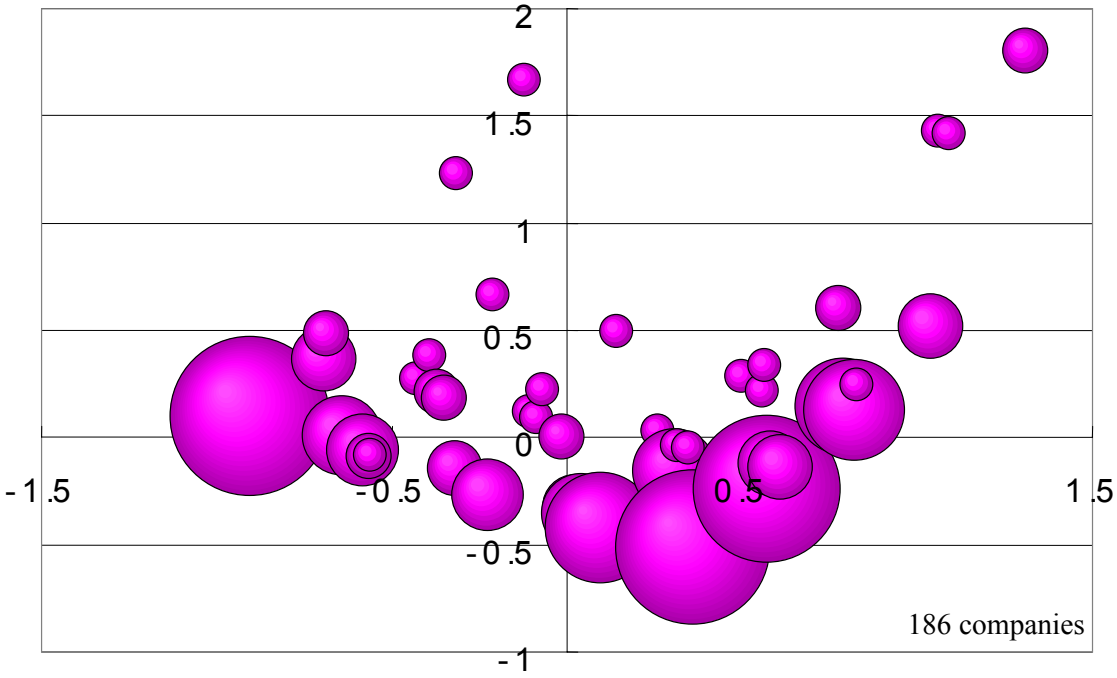


Figure 4 Status of IT proliferation in 1998

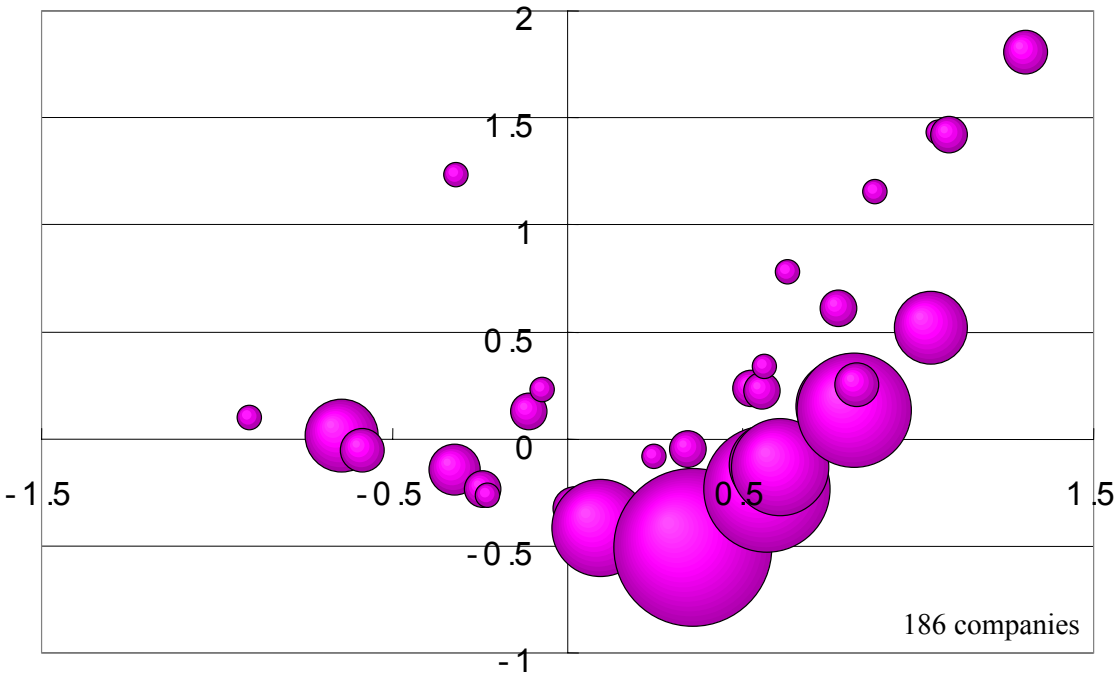


Figure 5 Status of IT proliferation in 2001

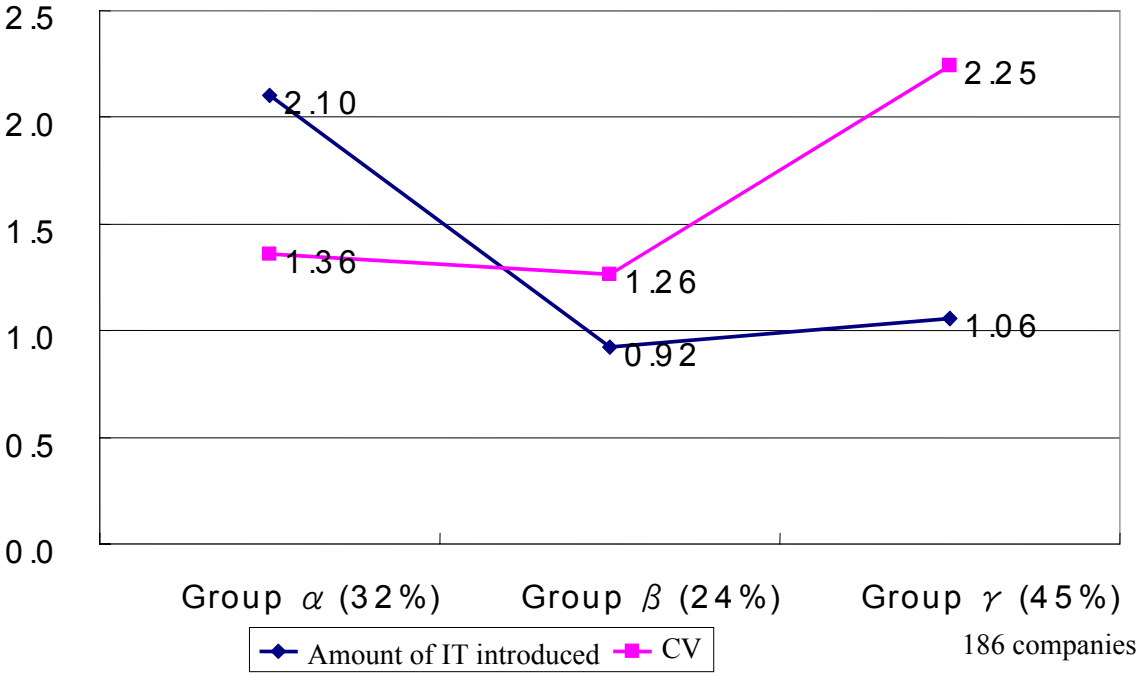


Figure 6 Pattern of IT introduction by corporate group

In 1995, the majority of respondents are concentrated in the third quadrant. This indicates that, at that stage, most companies had not yet introduced any of the eight types of IT surveyed on a company-wide scale. In 1996 and 1997, however, a growing proportion of companies were plotted towards the right half of the graph, thus indicating that the introduction of IT had begun.

In 1998, a large number of companies were plotted in the fourth quadrant, indicating that the introduction of IT, particularly that related to the Internet, moved forward in this period. In 1999, 2000 and 2001, the number of companies distributed in the first quadrant increased. This could be interpreted as an indication that companies that had completed the introduction of Internet-related IT up to a certain level are beginning to introduce non-Internet-related IT such as "videoconferencing systems."

Assuming that the annual difference in score shows the level of change in a company's introduction of IT, each company's respective introduction pattern was classifed, based on the total quantity of IT introduction (indicating the variety of IT introduced) between 1995 and 2001, and a coefficient of variation (CV: indicating the constancy of IT introduction in each year). The patterns that emerged from this classification could be roughly divided into the following three groups.[12]

As figure 6 indicates, 32 percent of those surveyed introduced more IT and had a smaller coefficient of variation—group ∂. Companies in this group had been active and constant in their introduction of IT. Similarly, 24 percent of respondents were classified as having introduced IT more slowly—group ß. Finally, 45 percent (group µ) had been inconsistent in that the level of IT introduction had varied widely from year to year.

Chief information officer (CIO)

In 41 percent of the companies surveyed, an executive officer has substantial responsibility for the establishment and operation of information systems, whereas in 54 percent, responsibility lies with middle management, who are in effect chief information officers (CIO).

Corporate culture

To determine the corporate culture of an organization, the companies were asked to assess themselves in comparison to 38 typical statements. For example, on management style and company emphasizes tradition and precedents. Using the Likert (five-point) scale, the trends illustrated in figure 7 emerged.

According to their self assessments, many companies recognized that they were in a rapidly changing environment, such as "capturing sales and costs data quickly is important" (78 percent), "environment surrounding industry and market changes rapidly" (72 percent), and "information systems are important to business" (61 percent). On the other hand, only a small number felt they were able to respond to changes in their surroundings, replying that they "have a high rate of mid-career recruitment" (13 percent), "adoption of employee originated ideas" (16 percent), "wages differ greatly depending on performance" (21 percent), "information on customers and market is shared by the whole organization" (22 percent), "good communication across departments" (23 percent), "work is often done in teams formed from multiple departments" (25 percent), and that they were "able to respond quickly to changes in their environment" (25 percent).[13]

A factor analysis of the results revealed three major factors that had a strong impact on corporate culture.[14] Factor 1 showed high scores for statements such as "top-down hierarchical management style" and "decisions are made quickly." Factor 2 indicates high scores for statements such as "tradition and precedents are considered important in decision-making" and

"procedure is an important part of decision-making." Factor 3 indicates high scores for statements such as "customer and market information is shared by the whole organization" and "customer and dealer opinion taken into consideration when formulating company policy." These factors may be summarized as follows:

Factor 1: a top-down hierarchical management style that places priority on speed;
Factor 2: a conservative corporate culture that places priority on procedure and precedents;
Factor 3: a priority on communication.

When the sample scores[15] of each company for each of these factors are plotted on a graph, taking factors 1 and 2 as the axes, most companies are concentrated in the second quadrant, which means that factors 1 and 2 are mutually exclusive. At the risk of being bold, generalizing factor 1 could be described as showing innovation and factor 2 as having a conservative corporate.

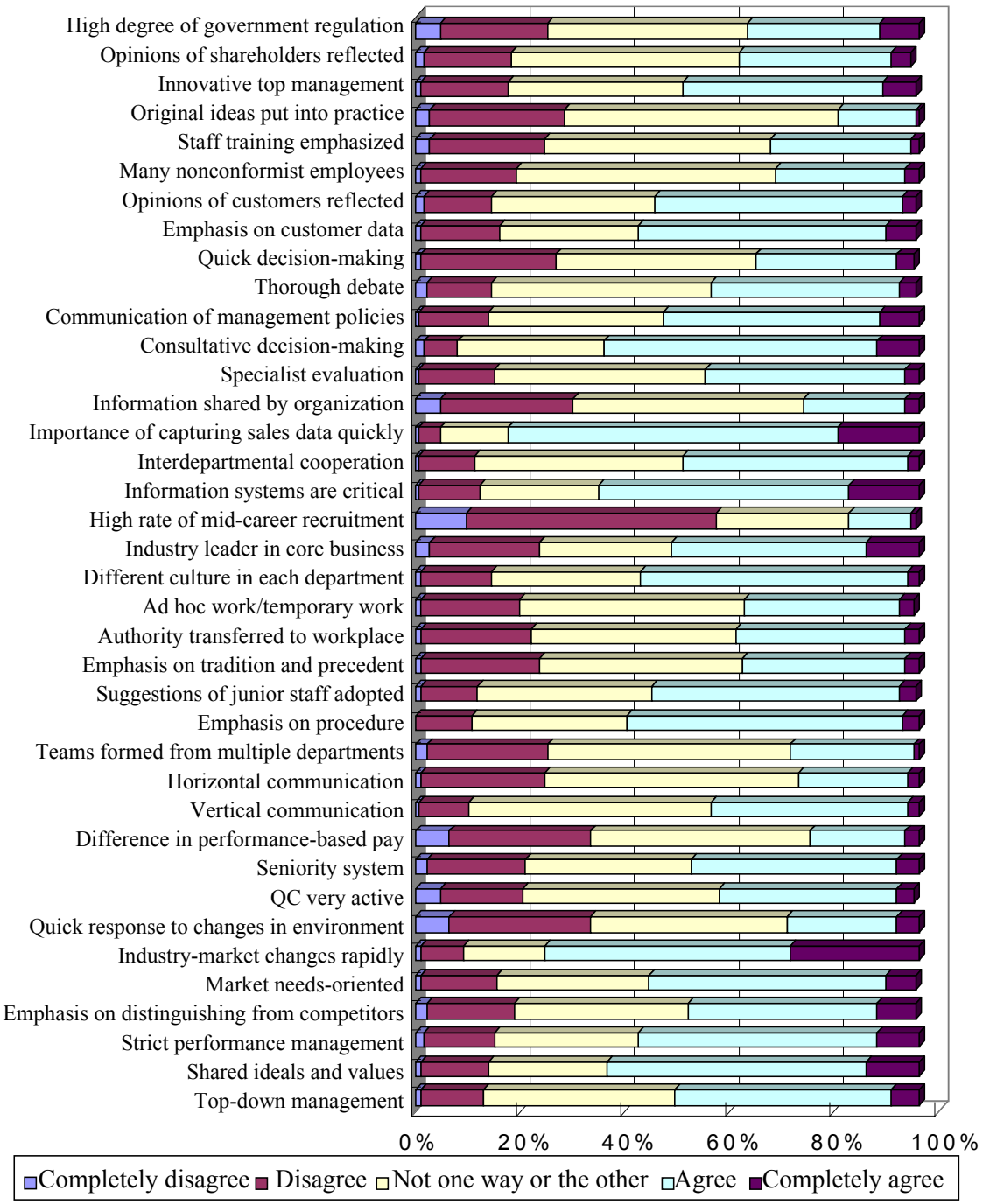


Figure 7 Corporate Culture

Classifying the companies using their sample scores for factors 1, 2 and 3 shows that they can be almost equally divided into two groups: those companies with a relatively conservative corporate culture (group I at 44 percent), and those with a relatively creative culture (group II at 45 percent).[16]

Hacking information systems

Current status

The survey revealed that 82 percent of those surveyed had experienced some form of illegal access of their systems. When examined by industry, the results also suggested that the financial industry was least likely to be adversely affected by illegal entry[17](figure 8).

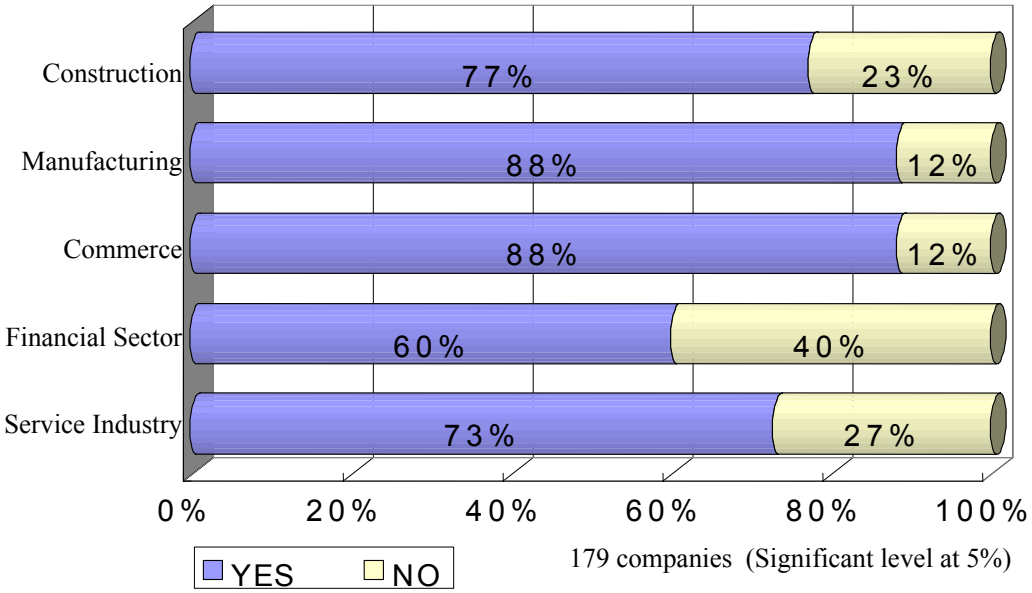


Figure 8 Experience of damage due to illegal access by industry

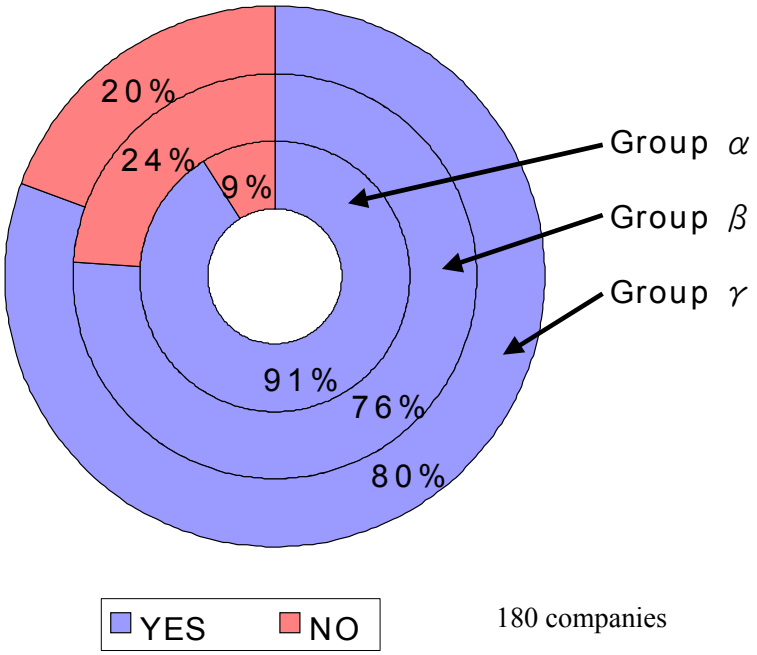


Figure 9 Damage from illegal access depending on way IT was introduced

When these results were examined against the company classifications of IT introduction patterns, it was apparent that companies in group μ, which had introduced vast quantities of IT were particularly prone to illegal access (figure 9).

Specifically, the overwhelming majority had experienced “computer viruses” (97 percent), followed by “attacks (attempts to obtain illegal access)” (27 percent) and “platform for sending spam mail” (21 percent), as can be seen in figure 10. Also, it should be noted that other types of illegal break-ins which could be extremely dangerous and cause serious damage, such as “email bombs” (7 percent), “email bugging” (3 percent) and “DoS attacks” (2 percent), were growing albeit only in small numbers.

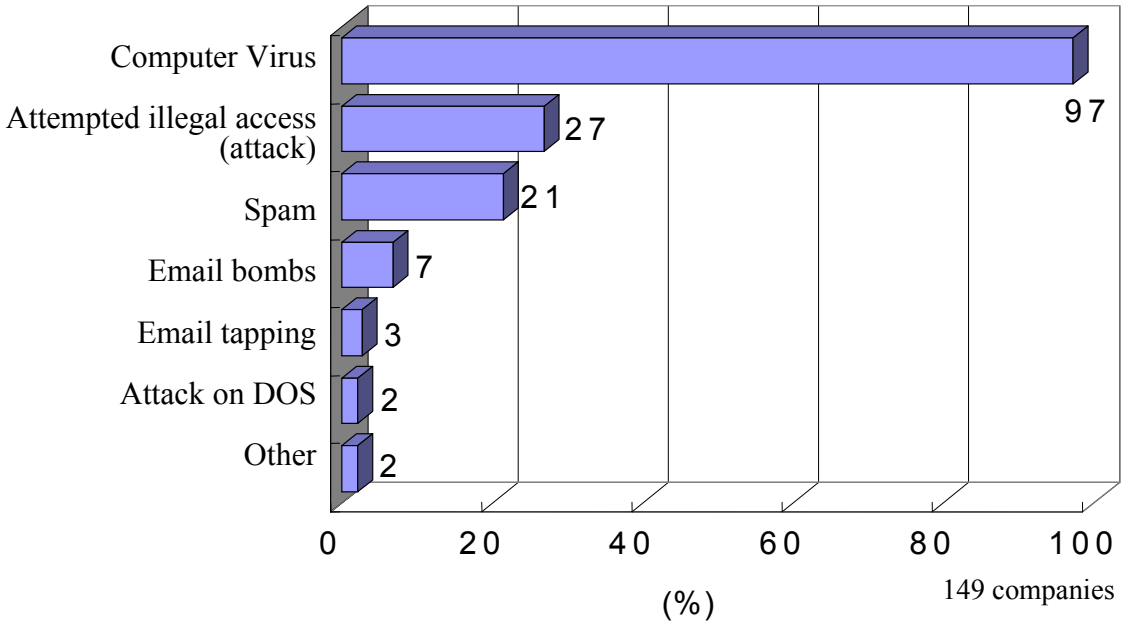


Figure 10 Type of illegal access

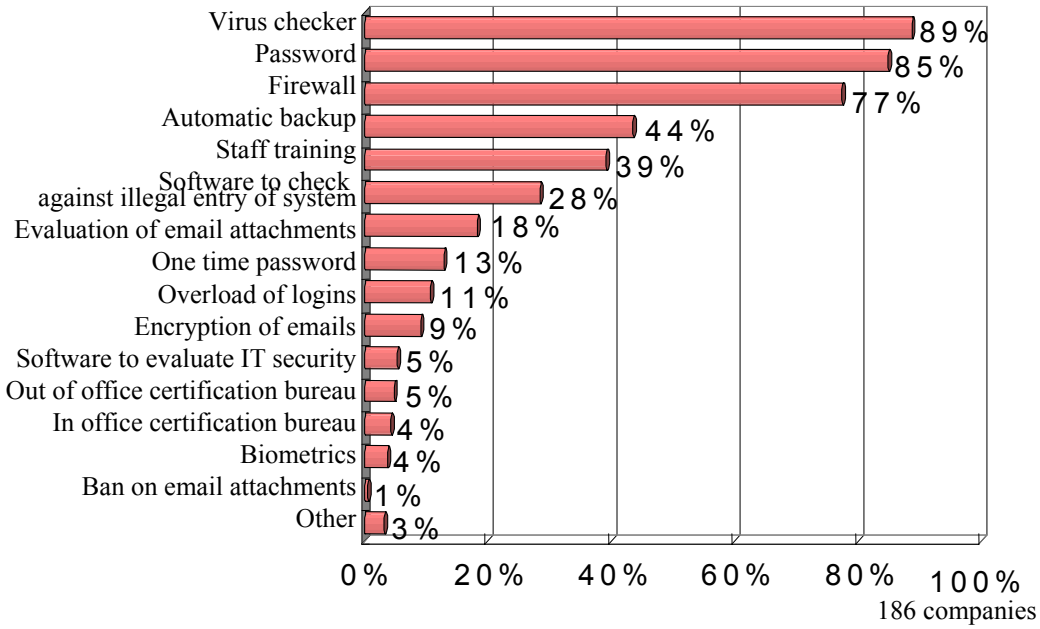


Figure 11 Measures against illegal entry

Measures against break-ins

Despite this situation, measures to protect company systems against illegal access were frighteningly inadequate (figure 11). Although most companies had adopted the three most typical measures, namely using "virus checker" software to protect computers from viruses (89 percent), the use of passwords (85 percent), and "firewalls" (77 percent), only 39 percent had considered staff training as an option.

Most companies seem to be relying too heavily on hardware such as "firewalls," software such as "virus checkers" and systems such as "passwords," while neglecting what in some respects is the most effective kind of countermeasure, namely "people measures."

In recent years, the number of companies adopting clearly defined policies on the use of computers and email and clearly defining employees' rights and obligations regarding computer resources is increasing.[18] In terms of people measures, it is very important that such policies, or e-policies, be clarified and disseminated thoroughly among employees.

According to this survey, however, only 38 percent of respondents had established their own e-policies. Moreover, one-third of these companies admitted that although they had the policies this did not necessarily mean that they would be observed. In reality, these e-policies only play a minor role in the fight against illegal break-ins, as can be seen in figure 12.

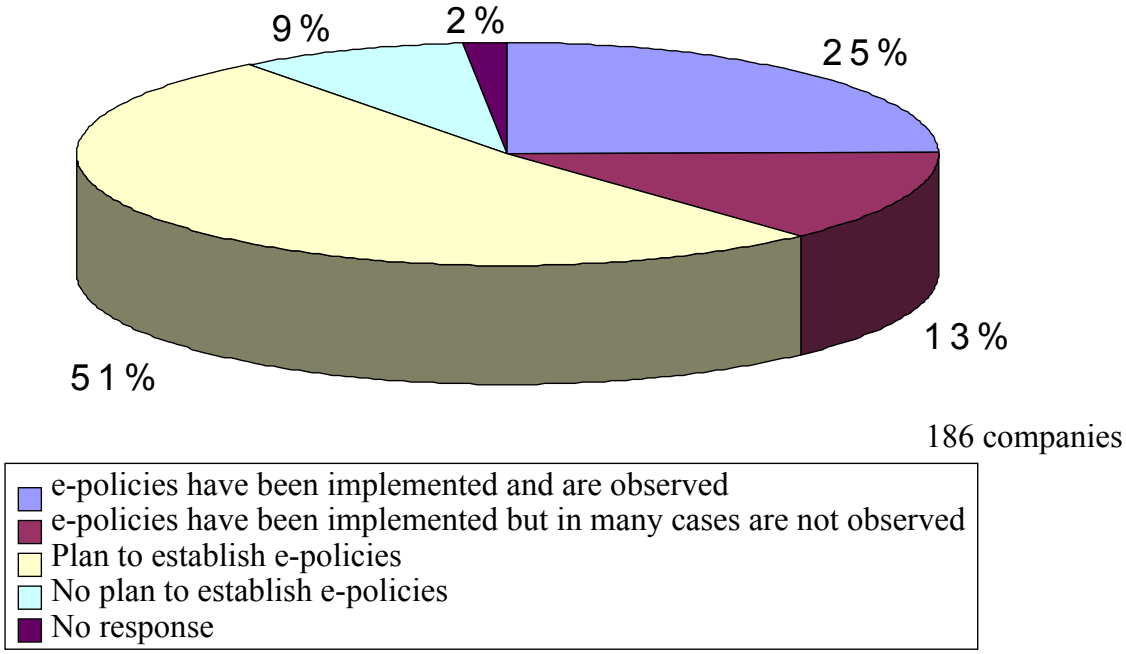


Figure 12 Implementation and observation of e-policies

The trends in the implementation and observation of e-policies vary significantly from industry to industry. Financial institutions have relatively high rates of implementing (57 percent) and observing (50 percent) e-policies. In contrast, less than 30 percent in the construction industry and the commercial sector had implemented an e- policy, and even when they had, they tended to be ineffective. Clearly, this is an area that many companies will need to improve.

Figure 13 shows the role a CIO plays in how well e-policies are observed, as the difference between the haves and have-nots is quite stunning. This proves that a strong leader with authority over the entire company is vital to build and operate an effective information system.

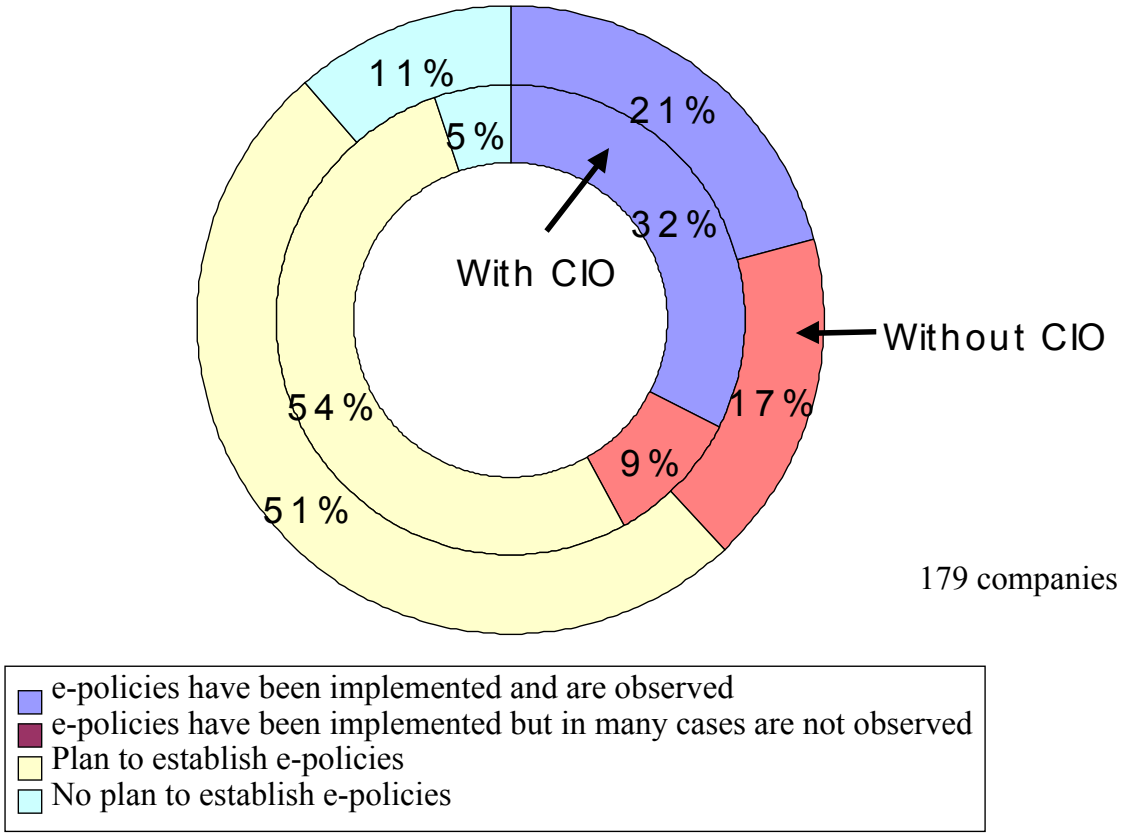


Figure 13 How e-policies are observed with or without a CIO

To prevent the leaking: controlling vital information

Another casualty of an illegal break-in into an IT network is the seepage of intelligence such as the leaking of customer detail or confidential information. While in most cases, illegal access is an external threat, the leak of internal information is more likely to be from within the company.

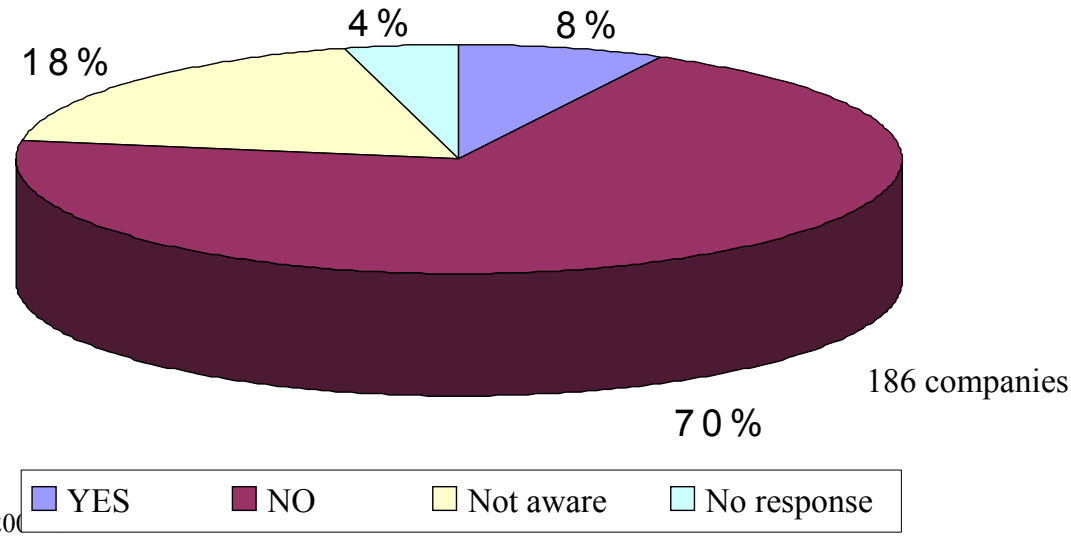


Figure 14 Experience of information leakage

Therefore, this issue is a slightly different question from the general problem of illegal access. According to the survey, only 8 percent had experienced leaks of important information (figure 14).

One clear difference between the havoc created by leaked information and the chaos created by an illegal access is that it is not immediately obvious when the former has happened. In fact, 18 percent of the companies surveyed admitted that they do not know whether information has been leaked. This makes it difficult to declare that most companies have never had confidential information leaked. Analysis by industry of the extent to which companies have experienced information leaks shows that, in sharp contrast to the results for illegal access, financial institutions have had far more incidences than any other industry. This may be due to the very nature of the financial sector, as they tend to be knowledge based, providing greater incentives for people to leak vital information. It may also be because financial institutions are more sensitive to leaked information than other businesses.[19]

Again, as figure 15 illustrates, the existence of a CIO makes a huge difference.[20] This is because many of the general measures adopted to prevent information leaking, including "limiting accessible information by each position and department" (75 percent), "information classified "confidential," "top secret," according to level and controlled accordingly" (44 percent), "number of computer terminals with access to vital information is limited" (36 percent), restrict employees' access to essential information. It is clear that the downside of such a policy is the hindrance to employee efficiency. In order for these measures to be effective, strong leadership over the whole company is a must (figure 16).

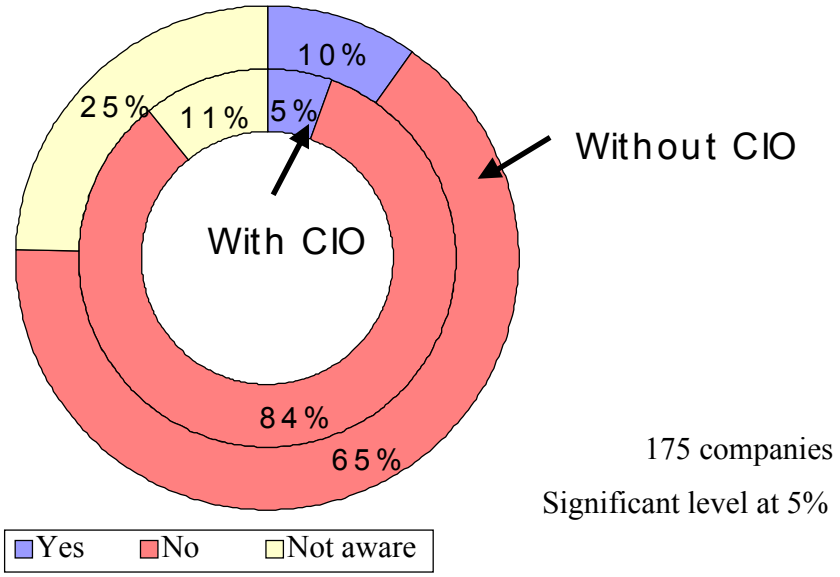


Figure 15 With and without a CIO: Experience of important information leaks

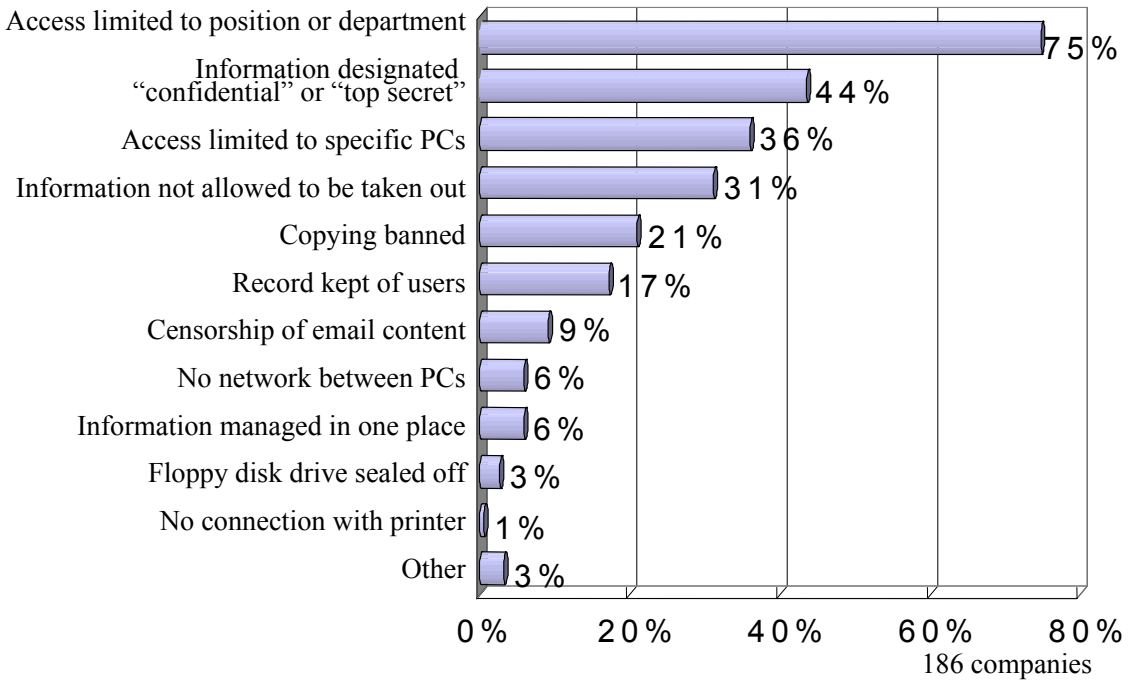


Figure 16 Measures against information leaks

Decision-making on information systems

Restrictions on implementing and managing information systems

The gist of section 3.4 was that general protective measures could have the adverse effect of hampering the work of employees. In general, when companies are building and operating information systems, a variety of restrictions are imposed which often turn out to be contradictory. In other words, the establishment of an information system is a decision-making process in which degrees of priority are attached to important factors under various restrictions. In this section, the most representative of those restrictions on employee efficiency, convenience to the customer and dealer, security, and cost are examined, as can be seen in figure 17.

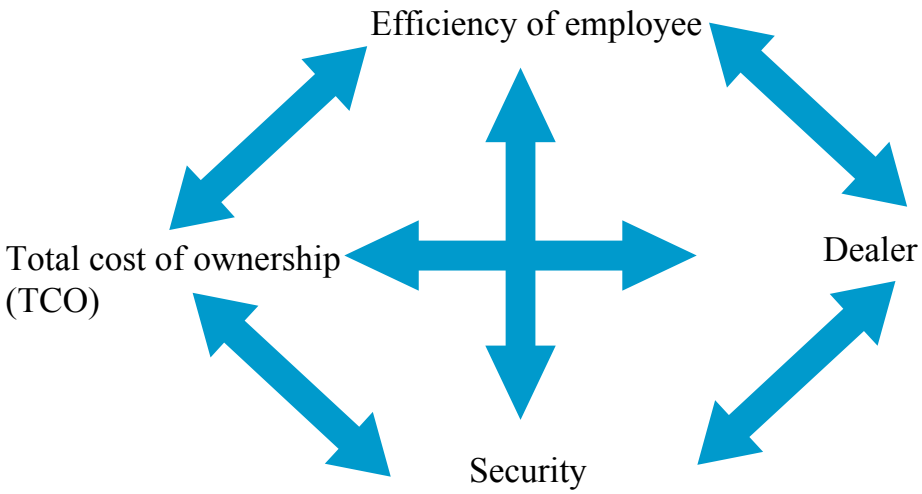


Figure 17 Examples of restrictions
on management and construction of Information systems

For example, for a company whose employees are often out of the office, if employees were able to access the company's Intranet from outside the office their efficiency would rise, but at the risk of endangering security. On the other hand, adding systems that are guaranteed to be safe to information systems would mean increased cost, thus imposing budgetary restrictions. Also, when customers demand information systems with high degrees of interoperability, companies will have to decide between the costs and the convenience of the customer and dealer.

As these examples show, mutually contradictory relationships exist between these four restrictions.

The conditions: show the priority

Companies balance these four restrictions in their information systems. Using an analytic hierarchy process (AHP), an attempt was made to find the criterion which companies considered important. Namely, the assessment criteria were presented in pairs (6 patterns), and the respondents were asked to assess the relative importance of one criterion over the other.

In figure 18, employee efficiency is compared to customer and business partner convenience. These results show that slightly more companies give priority to employee efficiency.

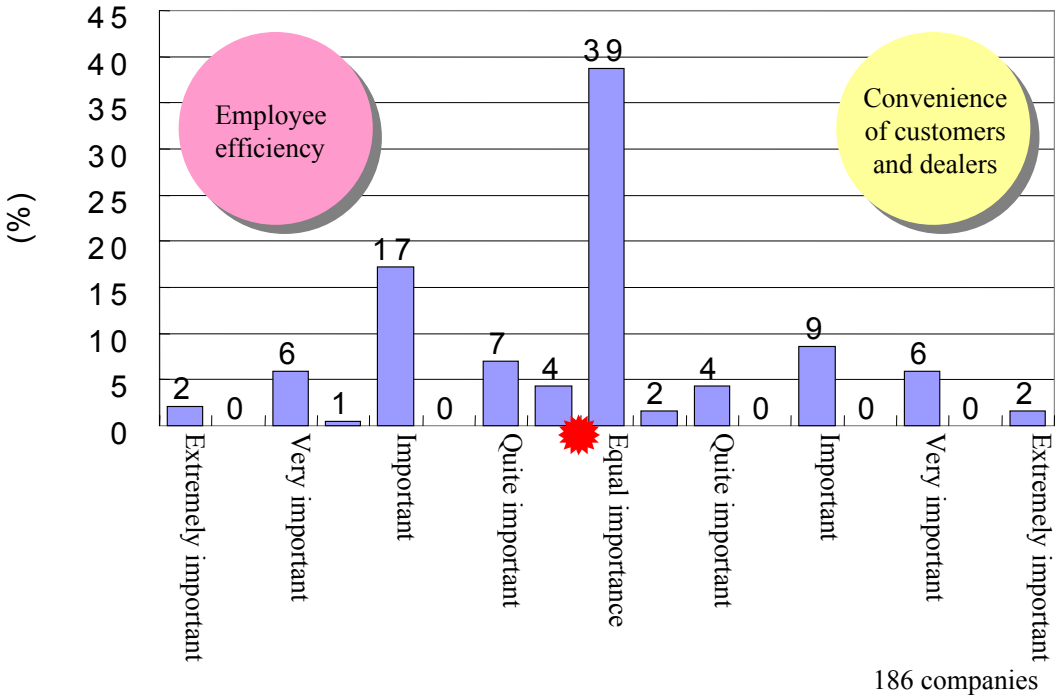


Figure 18 Employee efficiency versus convenience of customers and dealers

Figure 19 compares employee efficiency with security. Although the distribution is virtually equal, slightly more companies gave priority to security.

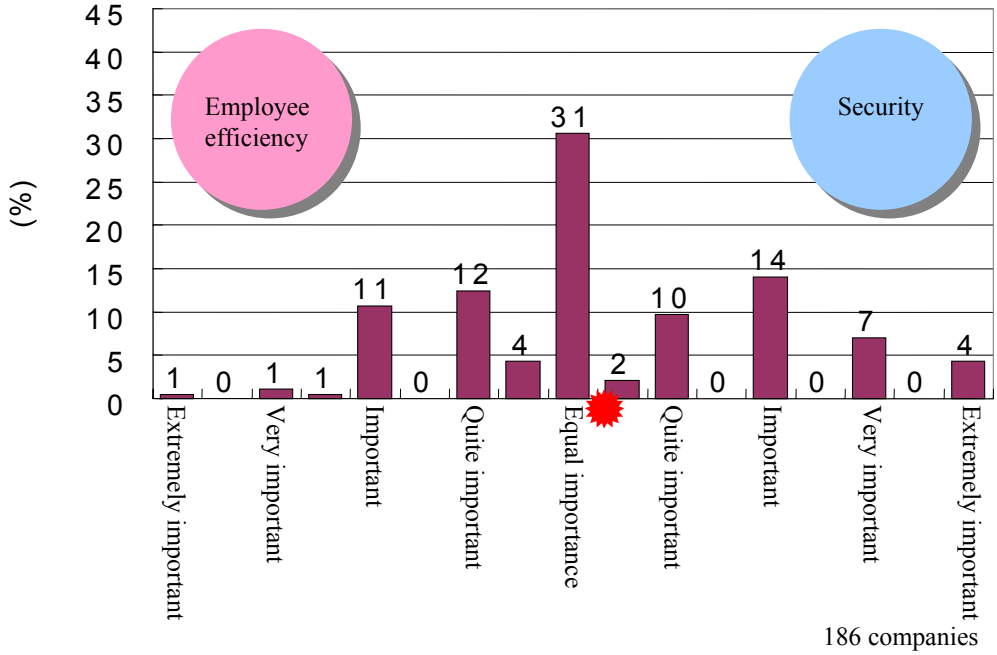


Figure 19 Employee efficiency versus security

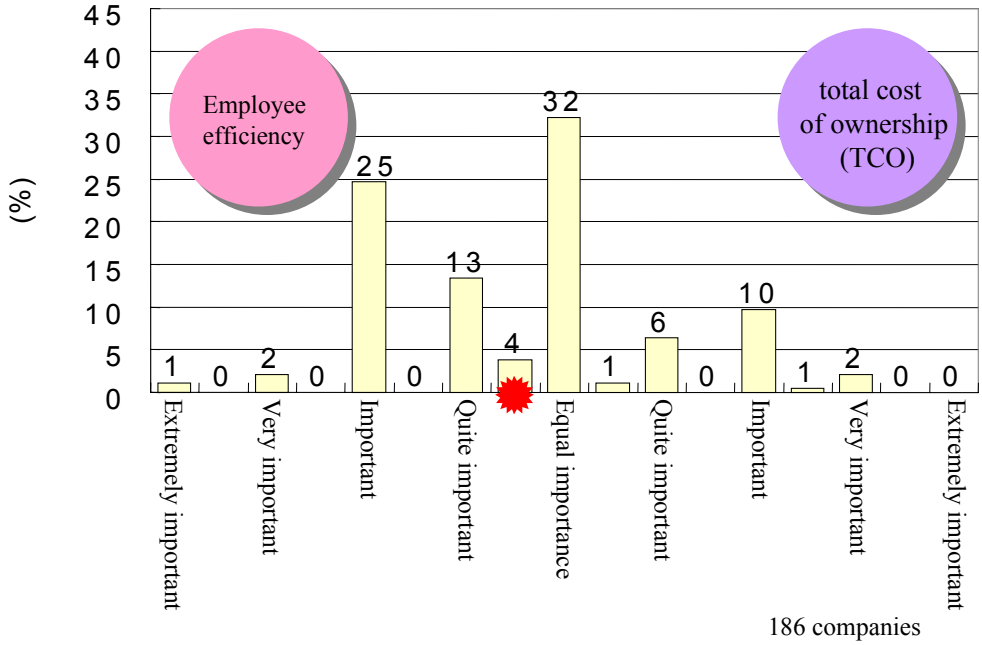


Figure 20 Employee efficiency versus versus total cost of ownership (TCO)

Figure 20 compares employee efficiency with cost, with efficiency being given priority.

Figure 21 compares the convenience of the customer and dealer with security; the latter was given priority.

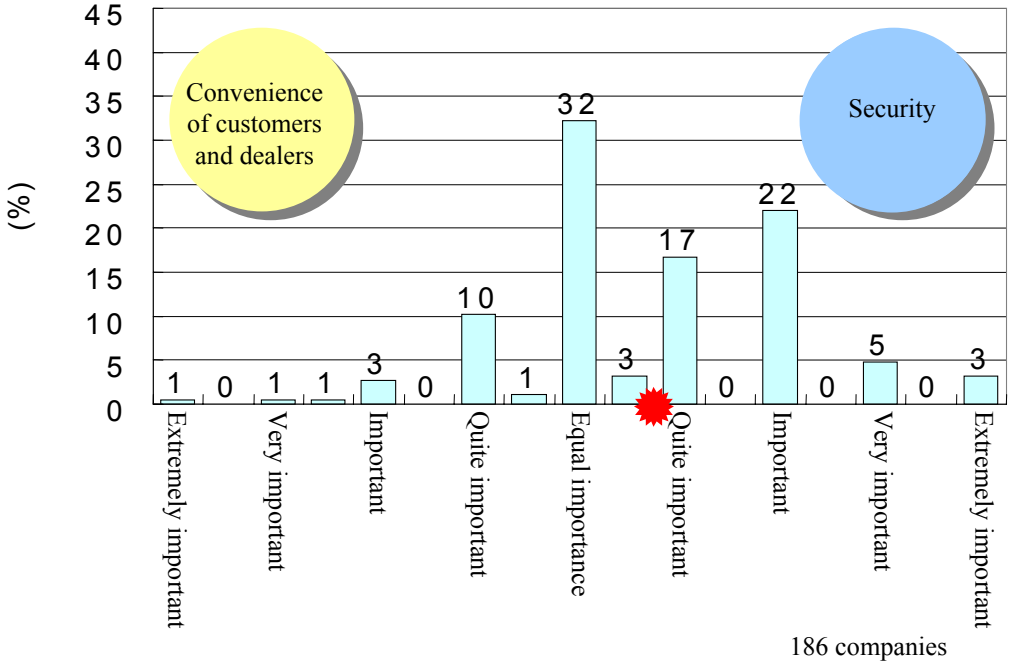


Figure 21 Convenience of customers and dealers versus security

Figure 22 compares the priority placed on convenience of the customer and dealer with TCO. The number of companies attaching priority to the former was considerably higher.

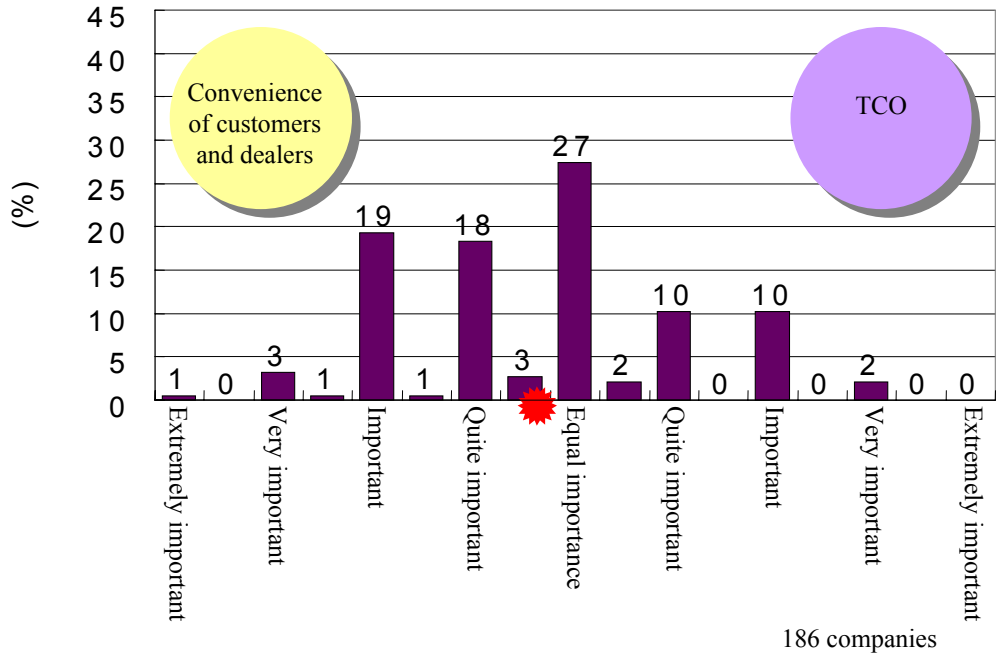


Figure 22 Convenience of customers and dealers versus TCO

Figure 23 compares security with costs, with an almost equal distribution, although security received slightly more responses.

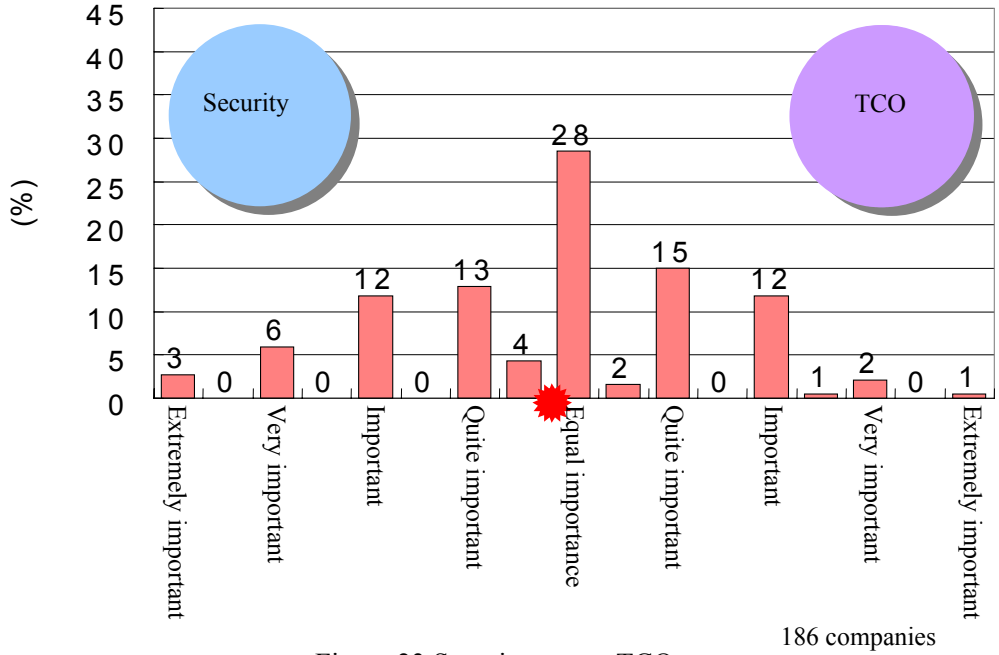


Figure 23 Security versus TCO

A value for each company was calculated by AHP on the basis of the above comparisons, and the correlation coefficients of the priority attached to these four restrictions were calculated. As shown in table 1, a strong negative correlation coefficient was observed between employee efficiency and security, and between security and cost. These results show the difficulties that companies face in choosing between these restrictions when building and operating information systems, and that striking a balance is their single greatest challenge.

Table 1 Priority attached to correlation coefficients

	Employee efficiency	Customer and dealer convenience	Security	TCO
Employee efficiency	1.00	-0.25	**-0.52**	-0.13
Customer and dealer convenience	-0.25	1.00	-0.28	-0.32
Security	**-0.52**	-0.28	1.00	**-0.46**
TCO	-0.13	-0.32	**-0.46**	1.00

The average value[21] for all respondents for the priority attached to the four restrictions[22] were 0.265 for employee efficiency, 0.222 for customer and dealer convenience, 0.302 for security and 0.212 for cost. Clearly, security is considered most important. Nevertheless, examining the distribution of companies in terms of the priority attached to each restriction, all four restrictions show a wide range of distribution, from companies that place a great deal of importance, to companies that almost completely ignore them, and each restriction shows a characteristic distribution trend.

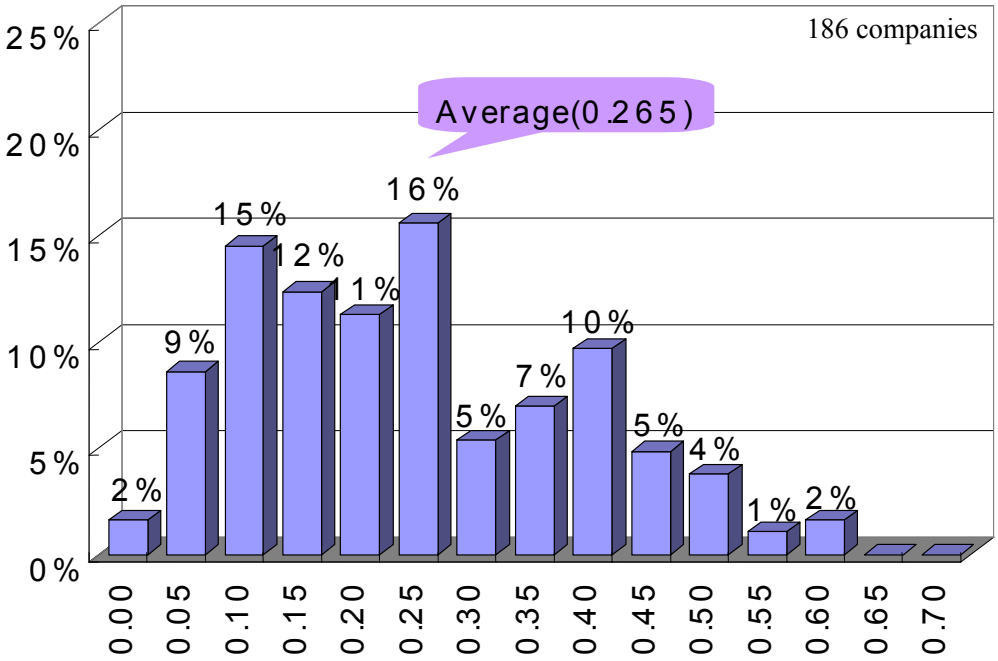


Figure 24 Weight distribution: rate of employee efficiency

For employee efficiency for example, the average value was 0.265, but many companies had weightings at the 0.10, 0.20 and 0.40 marks, and the kurtosis is a negative value of –0.616 (figure 24).

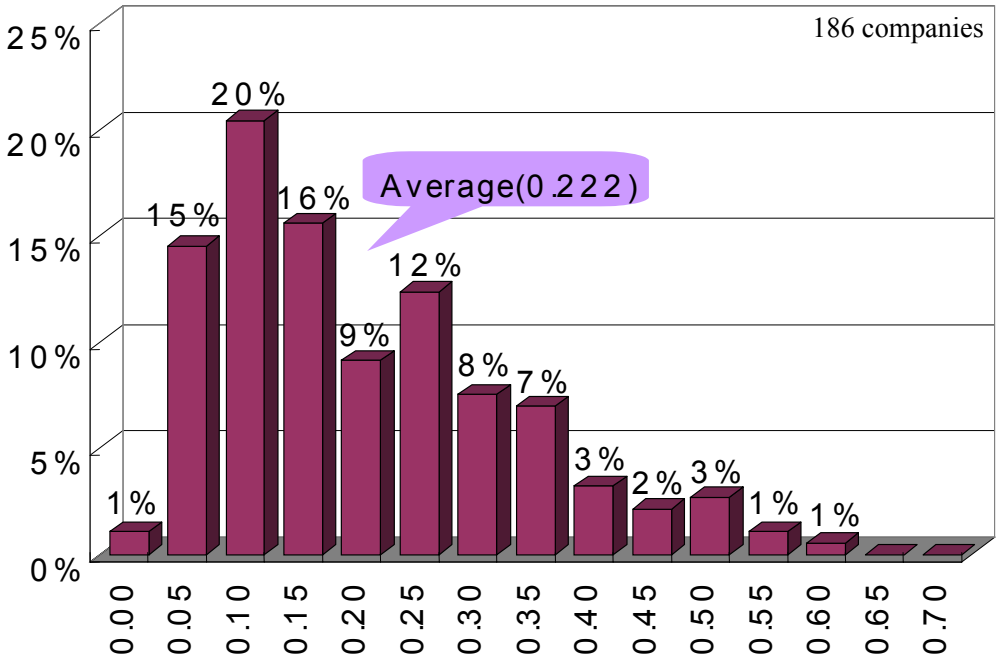


Figure 25 Weight distribution: rate of customer and dealer convenience

On the other hand, the average value placed on customer and dealer convenience was 0.222, but the priority attached to this restriction varied from company to company, with responses concentrated on the 0.10 and 0.25 marks (figure 25).

When these results are examined in terms of the IT introduction patterns described in the section on the introduction of IT, they show that companies in group α, formerly dedicated followers of IT, were not as equally dedicated to the convenience of their customers and dealers.[23] Companies in group α were clearly introducing IT more for their own sake than for others.

Security shows a markedly different pattern from the other three restrictions. The average value of security is quite high at 0.302. Many respondent companies are distributed around the 0.20 mark, but many companies gave this restriction a much greater weight than the average. 16 percent of companies attached a weight of 0.50 or more (figure 26), and its kurtosis was -0.361.

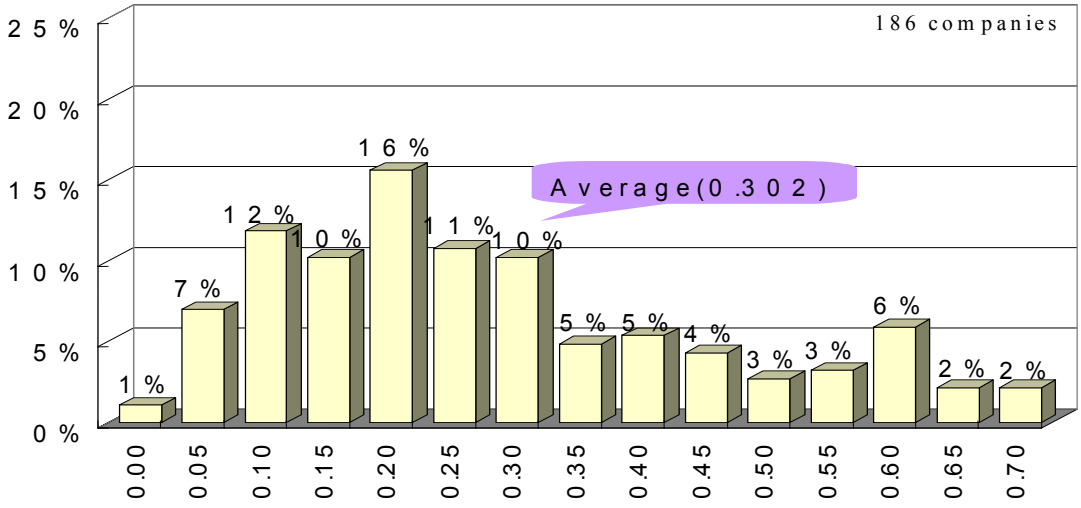


Figure 26 Weight distribution: rate of security

This does not necessarily mean that all respondents considered security to be an absolute necessity, but only that a certain number of companies considered security extremely important.

From the perspective of corporate culture, companies in group I, which tend to have a conservative environment, tend to be more dismissive of security concerns than those in group II, which have a relatively innovative corporate culture (figure 27).

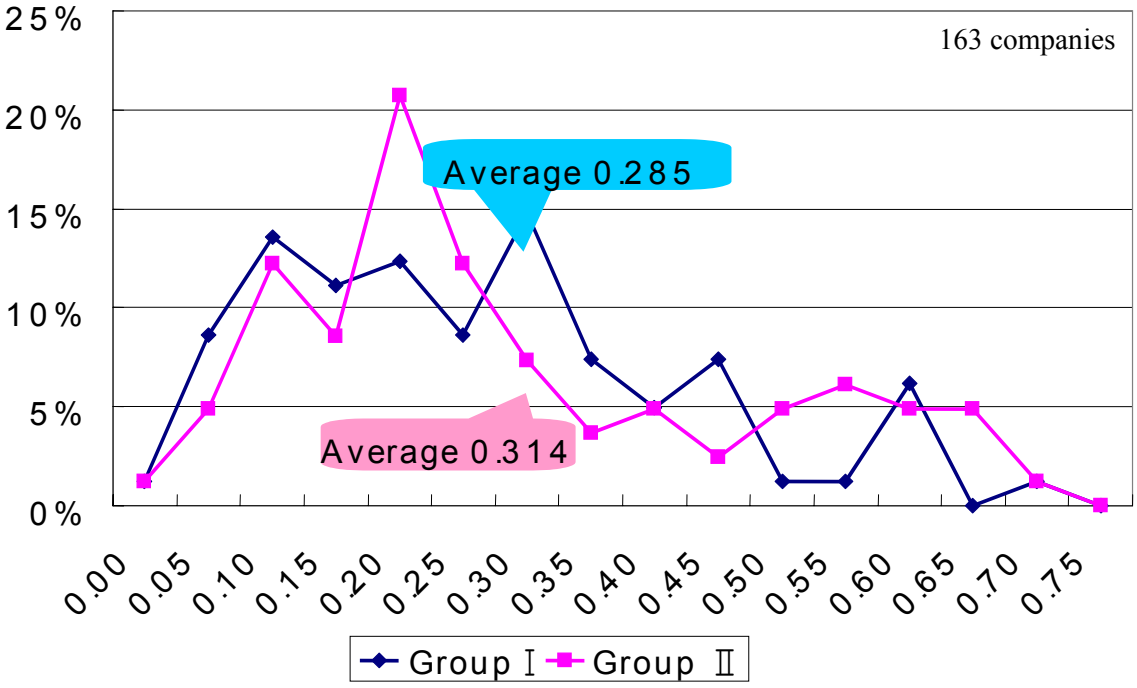


Figure 27 Weight distribution: rate of security from perspective of corporate culture

As for cost, although the average was 0.212, the distribution of scores formed an L shape, concentrating on the 0.10 mark. Both the kurtosis (0.570) and skewness (1.049) were high positive values (Figure 28). In addition, it is clear that cost is more important to companies in group I than those in group II (figure 29).

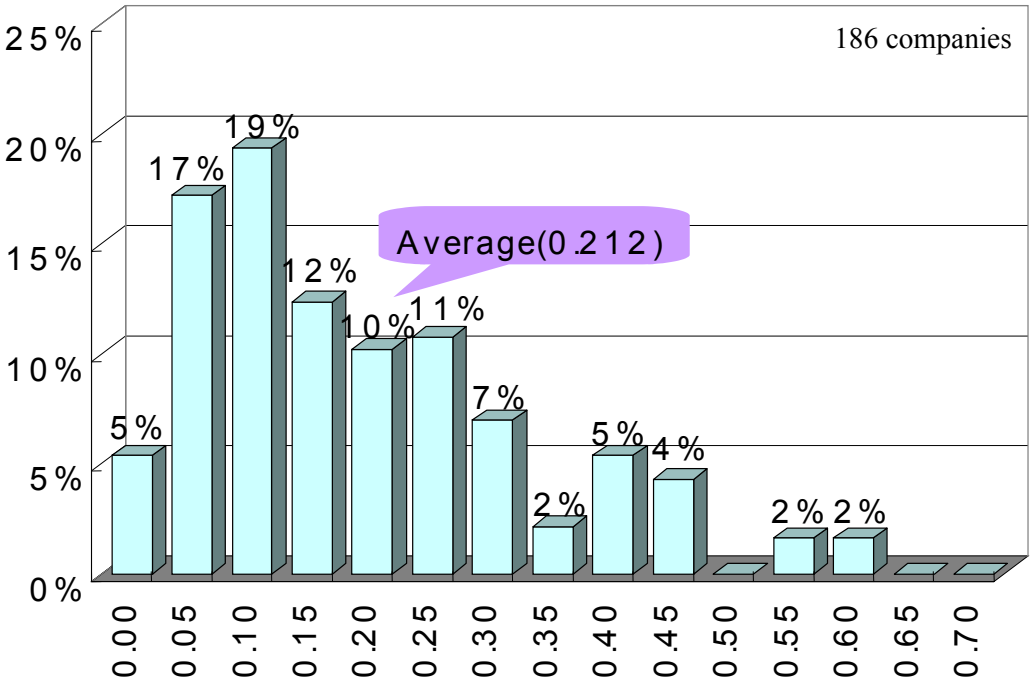


Figure 28 Weight distribution: rate of TCO

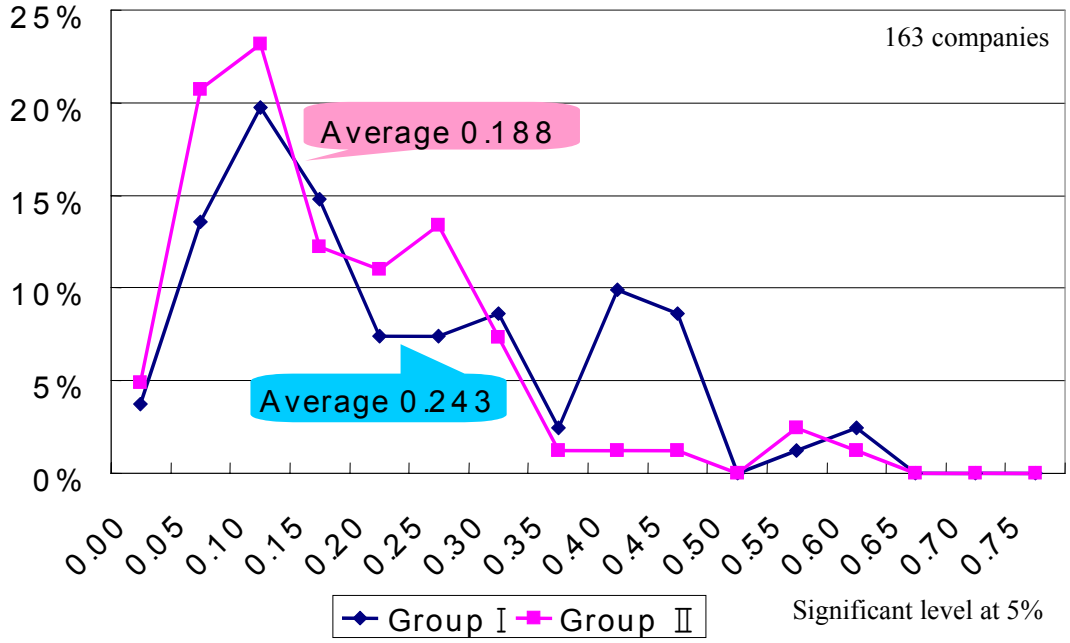


Figure 29 Weight distribution: rate of TCO from perspective of corporate culture

Also, as can be seen in figure 30, costs are considered more important in companies without a CIO than those with a CIO.[24]

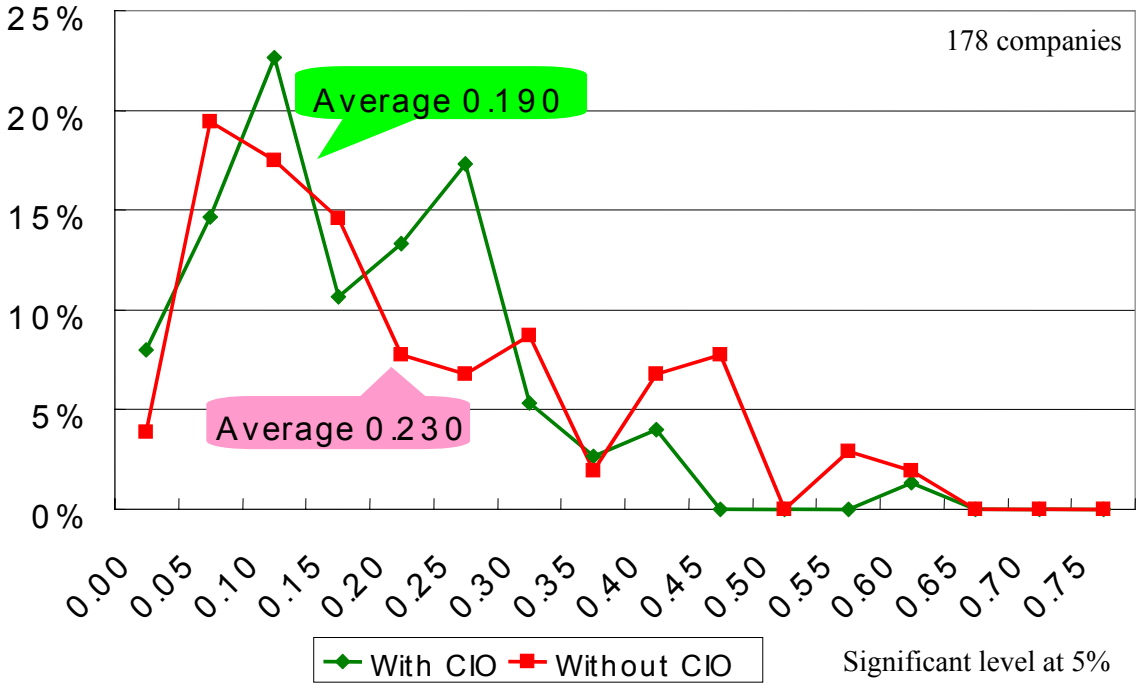


Figure 30 Weight distribution: rate of TCO with and without a CIO

As there was considerable variety in the respective importance attached to the four assessment criteria, the respondent companies can be broadly divided into four groups, depending on their weight scores.

Companies that regard employee efficiency (group U) as important account for 25 percent; 20 percent of companies surveyed value customer and dealer convenience (group C), and companies that attach importance to cost (group T) accounted for 28 percent. Only 24 percent (group S) placed security above other points, this group is not necessarily a majority group.

Figure 31 shows the scores (average value) for the priority attached to the four assessment criteria (restrictions) for each of the above groups.

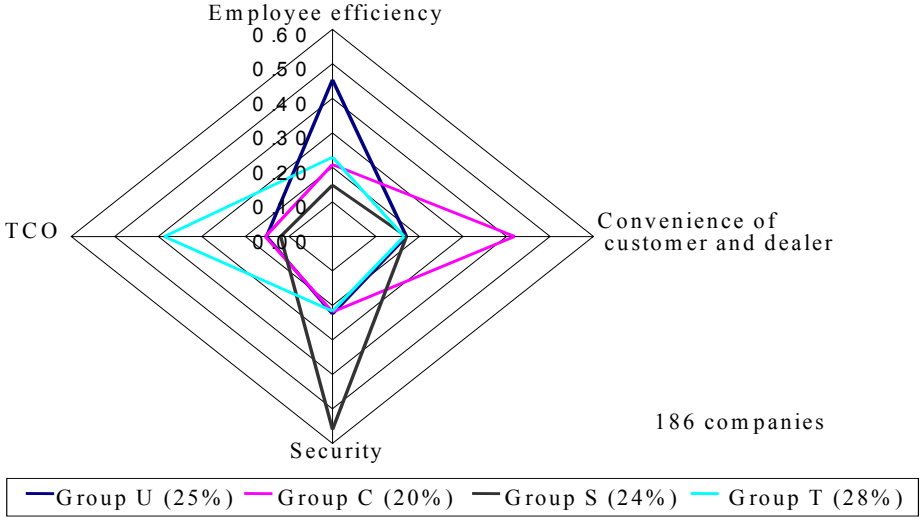


Figure 31 Type of organization depending on characteristics of weight distribution

Figure 32 shows that, when making decisions on information systems, companies give priority to only one of the four assessment criteria. Examined by business category, financial institutions tend to be classified in group S, (40 percent), group C has a large number of companies in the commercial sector (28 percent), and the service industry tend to be concentrated in group T (45 percent).

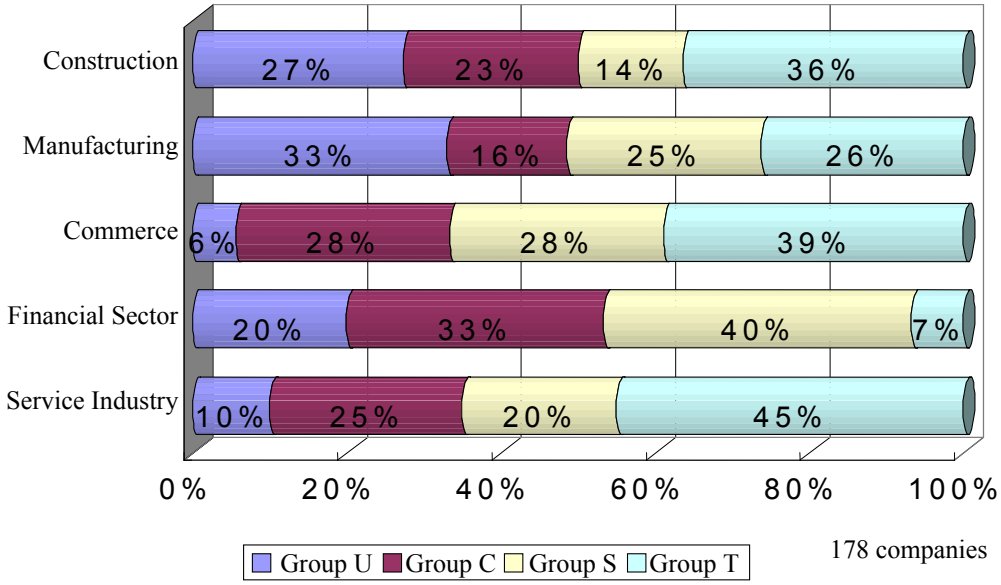


Figure 32 Type of organization depending
on characteristics of weight distribution by industry

The above analysis would suggest that conservative companies which emphasize precedents and procedures, and companies in which middle management is responsible for information systems, information systems are built and operated under strict budgetary constraints and other restrictions. This makes it difficult for such companies to spend their budgets flexibly on security, whose investment effectiveness is not readily visible.

Consistency of decision-making processes

As seen above, although each company has a different priority, this does not mean the decision was perfectly consistent or logical and in some cases, their assessments can be totally contradictory. Figure 33 indicates the distribution of consistency obtained by calculating the consistency index (CI.).

Kinoshita states that "if decisions are made with perfect consistency, the value of the CI is 0, whereas the larger the value, the greater the inconsistency will be," and "a CI of 0.1 or less (in some cases, 0.15 or less) would be acceptable."[25] Accordingly, the figure 33 shows that those companies that are consistently balanced in their construction and operation of information systems are far from being in the majority, and in many cases the decision-making process is prone to chaos.

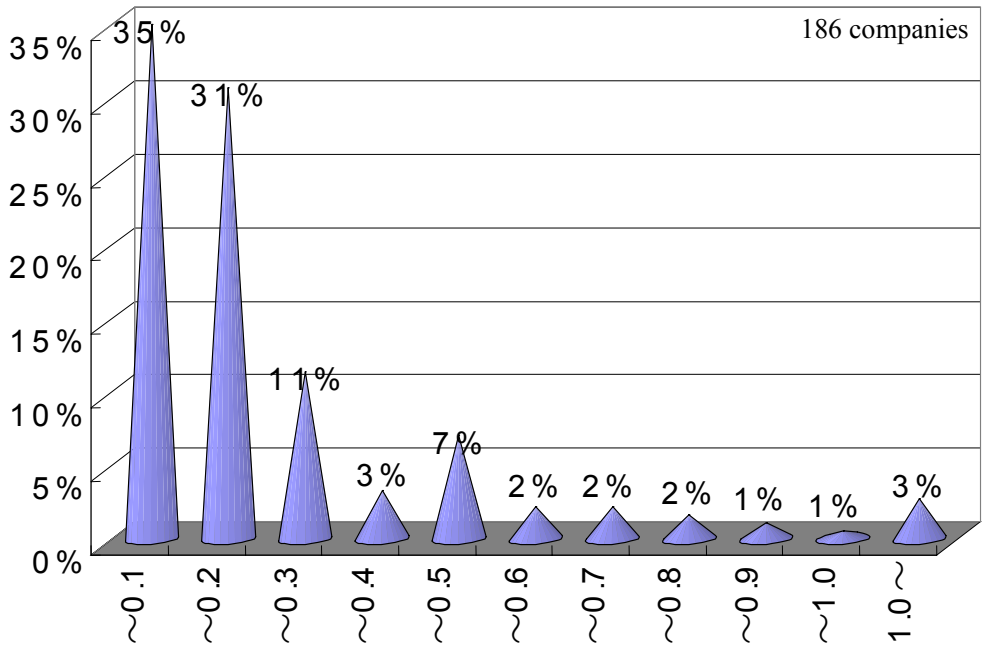


Figure 33 distribution of consistency obtained by consistency index (CI)

Applying this result to the company classification by IT introduction patterns, it emerges that companies belonging to group α (active IT introduction), have very high CI values.[26] Therefore, these companies, rather than installing information systems in a consistently logical manner, have done so for because of the excitement of the "IT revolution boom."

As was stated in the section on the introduction of IT, the reason that group α companies were so damaged from the illegal hacking of their systems was not only because they had introduced more IT than other groups, but also because such damage is a by-product of introducing IT without first setting out a clear decision-making procedure for information systems.

Conclusion

In this article, I have analyzed the various problems surrounding security management of corporate information, based on a survey of the major Japanese companies.

The results suggest that it is important to clarify who has managerial responsibility for information systems. On the whole, companies with a CIO tend to place greater importance on the security of their information systems, than those without a CIO, which seems to be quite effective. These companies are more likely to prioritize security over cost. On the other hand, if a company does not clarify that responsibility or leaves the responsibility at a junior level, it is only natural that cost should take priority over other conditions. In other words, such a company can only build and operate information systems within existing budgets.

This has implications for the systems of companies in which new, hitherto unforeseen dangers are starting to become apparent as information society progresses. At the same time, a conservative corporate culture where procedures and budget tend to have priority can be an

impediment to the management of information security. Inevitably, if IT is introduced without clear cut decisions this could lead to new risks for these companies.

Therefore, when companies introduce IT systems, it is important that delegation of responsibility in an organization is clear and decision-making processes are transparent.

They should not rush into decisions by an overly hasty commitment to the IT boom, but instead should conduct corporate reform at the same time.

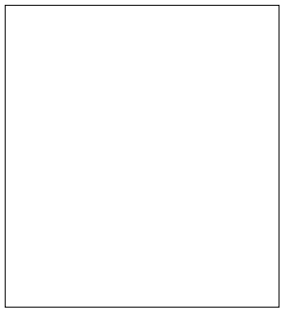
Notes

* This paper is a compilation of part of the findings of the "Survey on Corporate Risk Management in the Information Society," which was conducted with the assistance of The Telecommunications Advancement Foundation.

1 Japan Society of Security Management, *Security Handbook I* (Nikka Giren, 1998).
2 This involved the case of a disgruntled customer who posted his grievances on his website, which caused irreparable damage to Toshiba's public image.
3 Toshiaki Otsuka, *Corporate Security* (Tokyo: Diamond, 2001).
4 <http://www.cnhonker.com>
5 Harumi Yasui and Satoshi Ebitani, "Mushibamareru Kigyo Nettowa-ku" [Eroding Corporate Networks], *Nikkei Communications*, (Nikkei BP), 21 August 2000.
6 The government agencies whose websites were defaced during that week with statements about the Nanking Massacre were, in order of the extent of damage, the Science and Technology Agency, the Management and Coordination Agency, the National Institute for Research Advancement (NIRA), the Ministry of Transport, the Personnel Agency, the Government Data Research Center of Japan (GDRC), the Ministry of Posts and Telecommunications, etc.
7 On the same day, Bekkoame Internet, a major Japanese ISP (internet service provider), was inundated with 8x1056 emails in an "email bomb" attack, causing its mail server to crash.
8 Yasui and Ebitani, "Mushibamareru Kigyo Nettowa-ku" [Eroding Corporate Networks].
9 Osamu Inoue and Takuya Yoshida, "Domain Wars," Nikkei Computer, 15 January 2001, Nikkei BP.
10 The *Nikkei Kaisha Joho '99 (Natsu) Go* [Nikkei Company Data 1999 (Summer) Edition], Nihon Keizai Shimbunsha, was used for the selection of survey subjects.
11 The reason that an adequate valid response rate was not obtained is believed to be because the survey was not anonymous, and sensitive questions were asked such as the current state of corporate information security and information leaks.
12 By k-means cluster analysis.
13 These percentages are the percentages of respondents who replied, "strongly agree" and "agree" to the characteristics listed in the self-assessment on the Likert (5-point) scale.
14 Cumulative contribution of 0.383.
15 Score after varimax rotation.
16 K-means cluster analysis.
17 Significant at risk rate of 5 percent level
18 Michael R. Overly, trans. Toshiko Fujimoto, *ePolicy* (Tokyo: Nikkei BP, 2001)
19 This means that companies in other industries besides finance tend not to realize even if important information is leaked.
20 Significant at risk rate of 5 percent level
21 Arithmetical mean, not geometrical average
22 Standardised value so that the total value of the priority of all four assessment criteria equals 1.
23 Group α average: 0.20; Group β average: 0.24; Group γ average: 0.23. Significant at risk rate of 5 percent level
24 Significant at risk rate of 5 percent level
25 Eizo Kinoshita, *Nyumon AHP* [AHP for Beginners], (Tokyo: Nikka Giren 2000).

[26] Group α average: 0.30; Group β average: 0.20; Group γ average: 0.19. Significant at risk rate of 5 percent level

About the author



Akio Kunii is a Senior Research Fellow at the Institute for International Policy Studies. He has a BA in Education from the University of Tokyo, and an MBA. from Tsukuba University. Before coming to IIPS in August 1999, he worked as a researcher at InfoCom Research, Inc.; as a deputy research officer at the Institute for Posts and Telecommunications Policy of the Ministry of Posts and Telecommunications; and as a marketing manager at the Multimedia Service Promotion Headquarters of Nippon Telegraph and Telephone Corporation (NTT). His research at IIPS focuses on the influence of IT on social structures and management systems.