International Journal of Security and Its Applications
Vol.8, No.1 (2014), pp.201-212
http://dx.doi.org/10.14257/ijsia.2014.8.1.19

A Study of Security Requirement Demand Survey Analysis on Manufacturing Industry

Hangbae Chang[1]

Department of Business Administration, Sangmyung University
20, Hongjimun 2-gil, Jongno-gu, Seoul 110-743, Korea
hbchang@smu.ac.kr

Abstract

Countries across the world are showing interest on the investment of convergence industry amalgamated with IT according to the global economic crisis. For such convergence industry to become stable, it should be preceded by the establishment of environment for safely protecting cutting-edge technologies produced through IT convergence. However, cutting-edge technologies are being easily leaked outside as they become digitalized through IT convergence. However, existing studies have been mostly limited to information security centering on IT information asset. This paper conducted a study on the security requirement demand research for establishing response strategy on technology leakage possibility and leakage route by analyzing the business process of automobile industry. In conclusion, the biggest difficulty in sharing information of automobile industry was inability to inspect the status of technology protection of outside organization. Accordingly, the area of DB security is the security area that is thought to be most urgent as of now, and it was found in a research on the intention to introduce security system within 2 years that 66.7% of respondents are willing to introduce security system.

Keywords: *Demand Survey, Security Requirement, Manufacturing Industry, Automobile Industry*

1. Study Background

Global economic crisis and low growth lead to countries focusing on finding new investment channel for various new industries, along with manufacturing industry. Manufacturing industry has come into the spotlight as a new investment channel as convergence industry upon its amalgamation with IT. For such convergence industry to become stable, it should be preceded by the establishment of environment for safely protecting cutting-edge technologies produced through IT convergence.

In recent, technology protectionism is being spread in various countries across the world to strengthen national competitiveness by safely protecting the cutting-edge technologies with competitive edge. Technology protection is emerging as a new means to protect the country's own industry according to the increase of international treaties that prohibit protective trade, and various countries across the world are establishing national level strategies on technology transfer and technology sales for maximizing the profit from the standpoint of countries that possess technologies.

[1] Corresponding author
This research was supported by a 2013 Research Grant from Sangmyung University.

ISSN: 1738-9976 IJSIA
Copyright ⓒ 2014 SERSC

However, cutting-edge technologies that need to be safety protected are easily being leaked to competitors or abroad currently according to digitalization upon their amalgamation with IT, and number of according incidents and amount of damage are drastically increasing each year, thereby urgently requiring the establishment of strategy to protect cutting-edge technologies. For the purpose of preventing cutting-edge technology leakage incident, various countries across the world are making efforts to prevent technology leakage through various policy activities. However, number of industry technology leakage and scale of damage are not decreasing. In addition, basic environment such as organization specializing in security has not been properly established in companies except for some major corporation, and existing studies are limited to information security centering on IT information asset.

Meanwhile, business processes or construction processes of convergence industry vary according to each industry, and business processes are different even in the same industry. For technology protection, it is necessary to prepare response strategies on technology leakage possibility and leakage route that could occur in each area of business process according to industry. Instead of existing security system that consisted of each individual measure, it is necessary to establish convergence-based integrated security architecture from teleological aspect.

According, the purpose of this study is to conduct a study on security requirement demand research of manufacturing industry to apply security in the business process of convergence industry based on the limitation of current security activities of manufacturing industry and security solutions being used for fast-changing economy and technology. In specific, the purpose is to research security requirements based on business process to prevent technology leakage and verify the present condition of security of automobile industry that could affect national industry.

2. Preceding Studies on Security Requirements

In most studies, opinions of users are not being reflected in the researches on security requirements. In addition, the majority of studies are on analyzing only technical risk or deducing security threat and vulnerability during system development or against developed system only through preceding studies.

In Jung's study (2007), it proposed a methodology for deducing security requirements for developing protection profile (PP). The proposed methodology deduces threat that needs to be included in environment while creating PP through the risk analysis on each environment after dividing the environment into 3 levels. In addition, it packaged security objective and security functional requirements according to security environment by referring to documents used to develop PP in Japan and the US. Lastly, it presented guidelines for PP development in our country by proposed certified package according to environment.

In Jung's study (2011), it analyzed security threats that could occur in smart work environment and analyzed security requirements for safe smart work environment against various security threats.

In Kim's study (2012), it presented logical architecture that could be referenced while developing security requirements on charge infrastructure that will be established in various forms for safe electric car charge infrastructure. Based on the logical architecture presented, it identified security threats and security vulnerabilities that could occur. In addition, based on the importance of information exchanged in each interface, it presented security requirements for responding to identified security threats by dividing them according to confidentiality, integrity, availability, security

 Copyright ⓒ 2014 SERSC

prevention, certification and permission. In addition, it summarized and presented security measures against security vulnerabilities that could occur in system.

3. Empirical Analysis

3.1. Analysis of Automobile Industry Business Process

Development process in automobile area mainly consists of planning, styling, mock-up manufacturing, design (CAD modeling, blueprint creation) and prototype car manufacturing & testing.

Automobile product process mainly consists of core press (steel plate cutting & compression molding) ⇒ body assembly (press steel plate welding, assembly) ⇒ painting (body soundproofing, dust protection, anti-corrosion treatment & color painting) ⇒ designing (body interior/exterior & chassis assembly) ⇒ final test and core parts process such as engine and transmission based on passenger car.

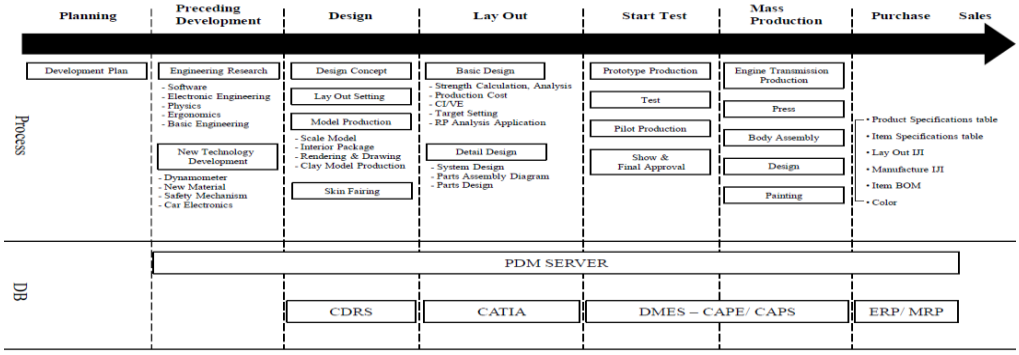

Figure 1. Automobile Industry Business Process

Basic construction process is a production process of engine and gears that leads to casting, forging, construction and assembly process to composed production system of one flow. Press construction process is a process of making panel for car exterior and steel plate warehoused in coil form is cut into desired size and pressed with press machine installed with mold to manufacture a certain shape of steel pieces (panel). As for body process, car shape is made by assembling and welding panels made through press process. As for painting of applying paint on car surface, its purpose includes material protection against rust or corrosion, enhancement and maintenance with beautiful color and differentiation from other models. Design process that is the final process in manufacturing car mainly consists of assembly and inspection process and it consists of main line where conveyor is assembled in flow work style and sub line of assembling parts unit.

3.2. Automobile Industry Security Status & Requirement Analysis and Research Design

For the purpose of researching the security status of automobile industry and analyzing security requirements, research was conducted through survey, interview, email and fax for major corporations and other small & medium enterprises (SMEs) with over 300 employees. The research survey was responded by 24 major corporations and 36 SMEs. In specific, 16 companies manufactured final finished product or according subsidiaries and 44 companies were partner companies.

Copyright ⓒ 2014 SERSC

For the purpose of analyzing the security status of automobile industry, research was conducted on technology leakage cases, information sharing status, establishment of security system in companies and according satisfaction level. For the purpose of researching the security requirement of automobile industry, research was conducted on difficulties in sharing information with outside companies, security system urgently needed to share information with outside companies, most urgent security area, intention to introduce security system within 2 year and type of system, area of long-term security system implementation, security technology to be introduced or developed in the future.

3.3. Analysis of Automobile Industry Security Status

Technology leakage cases showed that about 13.3% out of all responded companies experienced technology leakage. In specific, companies that manufacture final finished product & subsidiaries and partner companies occupied respective 50%, thereby showing that technology leakage is now occurring regardless of company type. It was found that technology leakage is gradually being spread from companies that manufacture final finished product to partner companies, and technological level of partner companies has improved to the point of being the object of leakage. Type of leaked technology was found to be design blueprint of product (100%) and pictures and images (25%) related to product sample for mass production for product being tested. As for the means of according technology leakage, portable storage device, email/messenger/web hard drive/P2P, printed materials, printouts, mobile phone camera, digital camera were being utilized, as shown in Table 1.

Table 1. Technology Leakage Means (Multiple responses)

			Email, Messenger, P2P, Web Hard Drive	Portable Storage Device	Laptop, PC take out	Server Connection from Outside	Malicious Code, Virus Hacking	Printed Materials, Printouts, Research Note	Mobile Phone, Digital Camera
Scale	Over 300 Employees N= 24	Frequency Percentage Inter rate	2 25.0 % 8.3%	4 50.0% 16.7%	-	-	-	2 25.0% 8.3%	2 25.0% 8.3%
	Less Than 300 Employees N= 36	Frequency Percentage Inter rate	-	-	-	-	-	-	-
Type	Manufacture & Subsidiary N= 16	Frequency Percentage Inter rate	-	2 25.0% 12.5%	-	-	-	2 25.0% 12.5%	2 25.0% 12.5%
	Partner Company N= 44	Frequency Percentage Inter rate	2 25.0 % 4.5%	2 25.0% 4.5%	-	-	-	-	-
Total N= 60		Frequency Percentage	2 25.0 %	4 50.0%				2 25.0%	2 25.0%

Copyright ⓒ 2014 SERSC

As for the means of sharing information within company among executives and staff members, shared folder in server was found to be the highest with 67.9%, as shown in Figure 2, with also high percentage of 17.9% for employee PC sharing. As for company scale, it showed the result of internal groupware & KMS (72.7%), shared folder within server (63.6%) and internal email or messenger (54.5%) for major corporations, whereas the result of SMEs was shared folder within server (70.6%), internal email or messenger (47.1%) and employee PC sharing (17.9%). It was found that percentage of shared folder within server was high regardless of company scale, thereby showing the need to reinforce its security.

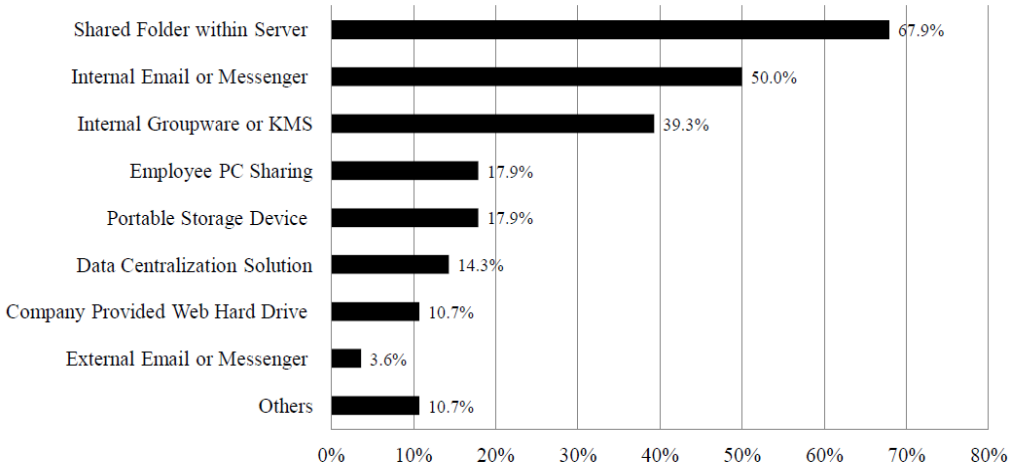

Figure 2. Information Sharing Means among Company Executives and Staff Members

As for means of sharing information with outside companies such as partner companies, 50% of respondents stated groupware or KMS account. As for company scale, percentage of information sharing with outside using printed materials and printouts was high in the case of major corporation, whereas percentage of information sharing through groupware or KMS account was high in the case of SMEs. In the case of SMEs, percentage of using email or messenger in the state of lack of data encryption was relatively high with 31.3%.

As for the information shared with outside, percentage of material & parts procurement was the highest (43.5%), while blueprint & BOM extraction (47.4%) was found to be vulnerable information against leakage. In the case of body design, it was found to be more vulnerable (26.3%) against technology leakage compared to sharing with outside (26.1%).

Copyright ⓒ 2014 SERSC

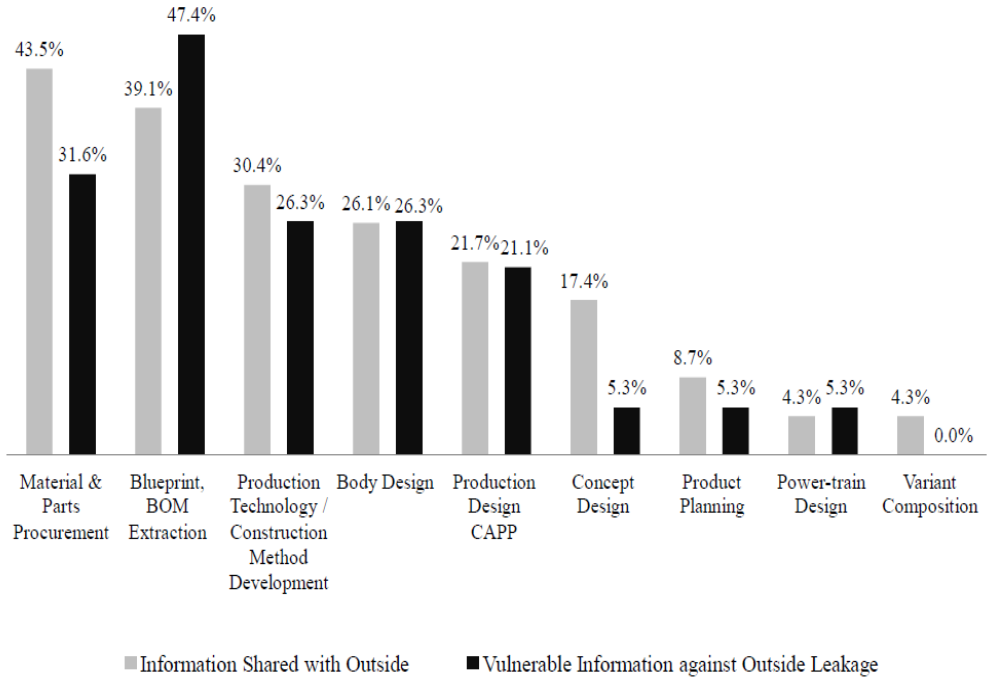

Figure 3. Comparison of Shared Information Type and Type of Vulnerable Information against Leakage in Automobile Area

As for the operation status of security system, it was found to be operated by all respondents. In regards to network security equipment in specific, network firewall was found to be the highest with 82.8%. As for security management system, log analysis management tool was found to be the highest with 68.4% while the use of security management system was found to be insufficient overall. In regards to PC security solution, the use of vaccine was found to be the highest. In the case of gate control system, control of gate through RFID or card showed the highest percentage with 89.3%. Lastly, in the case of the operation of information leakage prevention system, the percentage (61.5%) of portable storage device use control was found to be high. In the case of major corporations with over 300 employees, DRM, DB access control, portable storage device control and printout history surveillance showed the highest response rate with same percentage (54.5%). In the case of final finished product manufacturer & subsidiaries, the use of DRM, DB access control and portable storage device control (57.1%) were found to be significant to prevent information leakage. In the case of SMEs and part companies, on the other hand, implementation of data encryption solution such as DRM was insufficient, which is similar to the highest response percentage of data encryption technology such as DRM in urgently needed security system. In the case of SMEs and part companies, their percentage of DRM use is relatively lower than final finished product manufacturers, thereby showing their lower importance of operating DRM in connection to manufacturer and part companies.

Copyright ⓒ 2014 SERSC

Table 2. Present Condition of Information Leakage Prevention System Implementation (Multiple responses)

			DB Encryption	DRM	Data Centraliz-ation Solution	DB Access Control	DB Use History Surveillance	Portable Storage Device Control	Printout History Surveillance	DLP
Scale	Over 300 Employees N= 22	Frequency	6	12	6	12	2	12	12	4
		Percentage	273%	54.5%	27.3%	54.5%	9.1%	54.5%	54.5%	18.2 %
	Less Than 300 Employees N= 30	Frequency	6	-	2	8	-	20	10	2
		Percentage	20.0 %		6.7%	26.7%		66.7%	33.1%	6.7%
Type	Manufacture & Subsidiary N= 14	Frequency	4	8	6	8	-	8	6	-
		Percentage	28.6 %	57.1 %	42.9%	57.1%		57.1%	42.9%	
	Partner Company N= 38	Frequency	8	4	2	12	2	24	16	6
		Percentage	21.1 %	10.5 %	5.3%	31.6%	5.3%	63.2%	42.1%	15.8 %
Total N= 52		Frequency	12	12	8	20	2	32	22	6
		Percentage	23.1 %	23.1 %	15.4%	38.5%	3.8%	61.5%	42.3%	11.5 %

In regards to the satisfaction level comparison of security systems currently being operated, it showed low satisfaction level overall with further lower satisfaction level for security management and certified account management, application system security and information leakage prevention. In the case of major corporations, they showed lower than average satisfaction level in the areas of information leakage prevention, PC security and gate control, whereas SMEs showed higher than average results. This is closely related to the highest response rate shown for DB security and PC security as urgently needed areas of security, thereby showing the need to appropriately reflect the characteristics of major corporations. In addition, the reason for high satisfaction level of SMEs is thought to be from the fact that they can easily apply the above security systems for SMEs. In the case of final finished product manufacturer & subsidiaries, they showed relatively lower than average satisfaction level in the area of information leakage prevention, as they responded to a field research that their plan and schedule are interrupted because security solution such as DRM do not support development & production related system and application. In the case of design system, for example, they responded that their work load increases as it supports 64bit while DRM is 32bit. In the case of part companies, they showed low satisfaction level overall and they showed very low satisfaction level in certified account management system and application system, which was found to be dissatisfaction from the need to implement various solutions due to lack to integrated security solution suitable for SMEs.

Copyright ⓒ 2014 SERSC

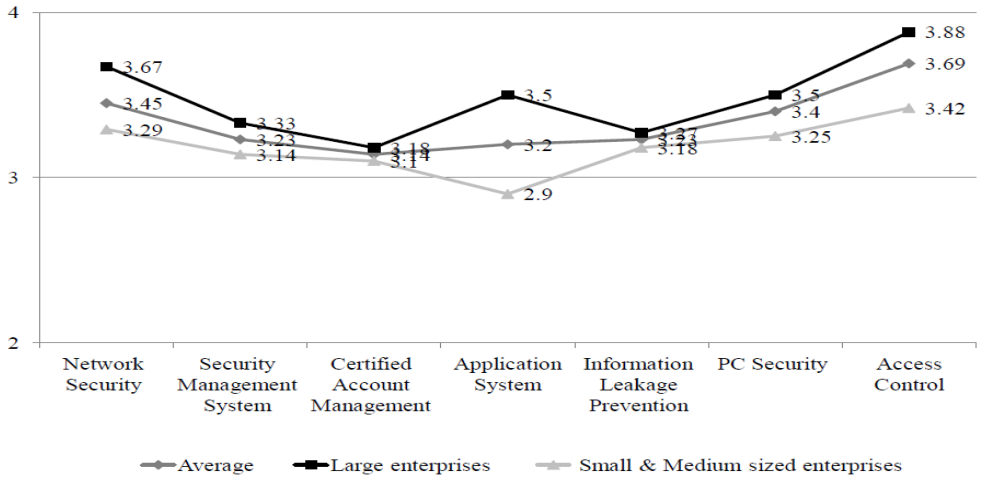

Figure 4. Satisfaction Level of Security System Currently Being Operated per Company Size

3.4. Automobile Industry Security Requirements Analysis

As for the biggest difficulty in sharing information with outside companies, the response of not being able to inspect the technology protection status of outside companies was found to be the highest with 34.6%. As for difficulties in information sharing per company size, the biggest difficulty for major corporations was technology protection surveillance and control for part companies (58.3%), whereas the biggest difficulty for SMEs was lack of data encryption solution installation such as DRM and lack of log record of system and date access and printout (35.7% for each). In regards to priority measures needed for SMEs to share information with outside, they were found to be information access right & log record, encryption/decryption right setup document management system and DRM solution installation.

As for security system implemented to share information with outside companies, they responded in the order of partner support center (37.5%), VPN or private network (33.3%) and data encryption solution such as DRM (33.3%). In regards to security system implemented to share information with outside according to company size, the response of data encryption solution such as DRM (66.7%) was the highest for major corporations, whereas the response of partner support center (41.7%) was high for SMEs. Such phenomenon was also shown according to company type. As for security system for sharing information with outside partner companies, VPN or private network implementation and active directory showed high response rate of respectively 31.3%, thereby showing that they prefer private network with main contractor and server terminal type PC security.

 Copyright ⓒ 2014 SERSC

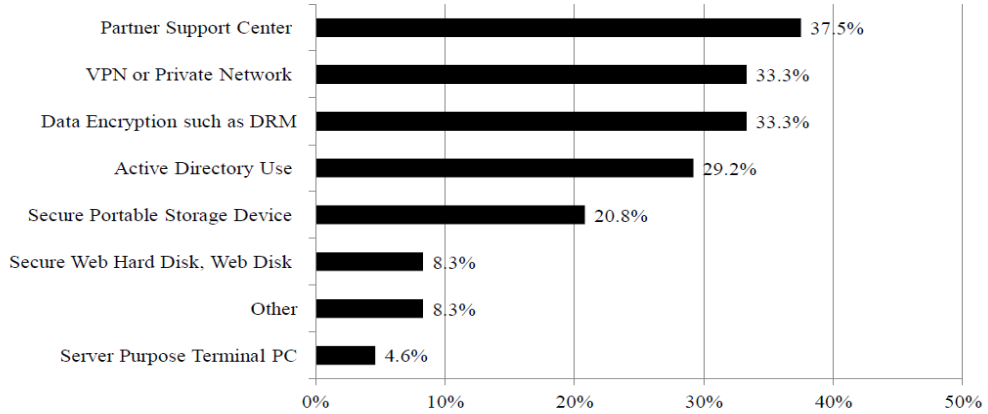

Figure 5. Information Sharing Difficulty with Outside Companies

In regards to most urgently needed security system for sharing information without outside companies, data encryption solution such as DRM (19.6%) was found to be the highest. As for the response measure against the difficulty in inspecting the technology protection of outside company while sharing information outside, it was found that they chose encryption of data instead of its control. The ROI of security control & monitoring and the ROI of data encryption solution such as DRM were compared and the result showed that the latter was efficient.

As for the security area considered to be most urgently needed currently, 41.4% of respondents stated DB security area followed by partner company security (31.0%), PC security (27.6%) and staff security (24.1%). According to the security system urgently needed that was analyzed earlier, it showed a similar pattern of data encryption such as DRM, detection of important data storage inside PC, tracing technology and security data center. It is though that importance of data is higher than other area, and it would be necessary to develop technology for preventing any occurrence of data leakage from outside, along with weight reduction of data security centered security solution.

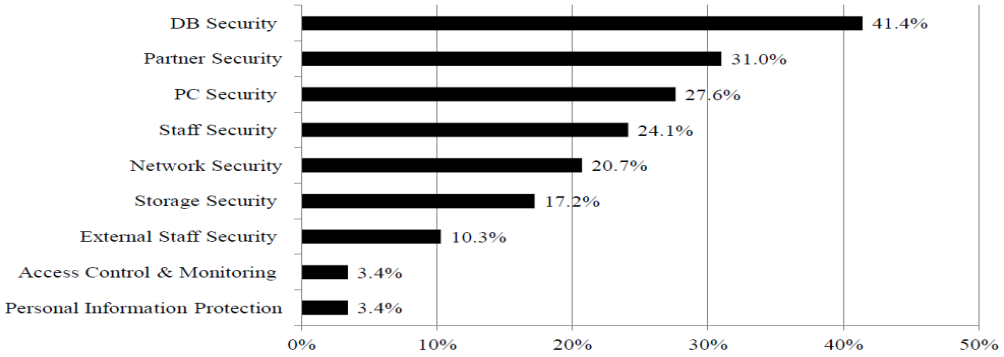

Figure 6. Security Area Most Urgently Needed Currently

As for the willingness of implement security system within 2 years, 66.7% of respondents stated that they are willing to implement. In regards to the willingness to

Copyright ⓒ 2014 SERSC

implement security system per area within 2 years, 70.0% of respondents stated information leakage prevention system. As for security area that requires long-term implementation, data centralization solution was the highest with 33.3% followed by integrated PC security (23.3%), early warning for risk analysis or integrated control (13.3%). The focus is on data security, and in the case of integrated PC security, it was considered as the second best plan of data centralization solution. In the case of early warning for risk analysis and integrated control, it was found that there is a need from the access control & risk management level according to data centralization. This was found to be the intention to reinforce security while focusing on company's productivity by reducing the costs that occur from data control through various security solutions. In regards to the reason for the high response rate of SMEs and partner companies on early warning for risk analysis and security control, it is because they prefer integrated security management rather than paying attention individually from functional dispersion.

As for security technology that needs to be implemented or developed in the future, expandable DRM solution that supports various applications that prevent secondary duplication showed the highest percentage (50.0%). It was found in the order of technology for automatically deleting data while only leaving tracking trace in environment where agent is not installed (36.7%), data centralization solution (30.0%) and illegal data detection technology (30.0%). As data security is consistently emphasized in automobile area, it is expected that demand will increase for DB security or prevention & tracking of information leakage in the future in the area of security technology development. In particular, there is a need to alleviate the burden through weight reduction of security area of user's usage by developing technology of data centralization solution such as SBC (Server Base Computing), and connect it to productivity improvement. According to company size, it was found that major corporations prefer virtual data centralization & network separation technology, whereas SMEs prefer technology of automatic deletion while only leaving tracking trace in environment where agent is not installed. While there is a demand for advanced prevention such as data centralization and leakage route control among major corporations, it was found that there is a demand among SMEs for response after leakage.

4. Conclusion

Currently, cutting-edge technologies that need to be safety protected are easily being leaked to competitors or abroad currently according to digitalization upon their amalgamation with IT, and number of according incidents and amount of damage are drastically increasing each year, thereby urgently requiring the establishment of strategy to protect cutting-edge technologies. For the purpose of preventing cutting-edge technology leakage incident, various countries across the world are making efforts to prevent technology leakage, but number of industry technology leakage and scale of damage are not decreasing. In addition, basic environment such as organization specializing in security has not been properly established in companies except for some major corporation, and existing studies are limited to information security centering on IT information asset.

This paper conducted a study on the security requirement demand research for establishing response strategy on technology leakage possibility and leakage route by analyzing the business process of automobile industry.

 Copyright ⓒ 2014 SERSC

In conclusion, the biggest difficulty in sharing information of automobile industry was inability to inspect the status of technology protection of outside organization. Accordingly, the area of DB security is the security area that is thought to be most urgent as of now, and it was found in a research on the intention to introduce security system within 2 years that 66.7% of respondents are willing to introduce security system.

As for future study, study on contact point security per industry and security study of each industry will be conducted by analyzing the business process of each industry.

References

[1] W. Chiu, R. Deng, C. Chang and S. Chen, "Development of digital convergence service industry: An analysis of cross-country comparisons", Service Systems and Service Management (ICSSSM), 2013 10th International Conference on 2013, IEEE, **(2013)**, pp. 607-612.
[2] M. S. Idrees, G. Serme, Y. Roudier, A. S. De Oliveira, H. Grall and M. Südhol, "Evolving security requirements in multi-layered service-oriented-architectures", Data Privacy Management and Autonomous Spontaneus Security, vol. 7122, **(2012)**, pp. 190-205.
[3] B. Jung, I. Han and S. Lee, "Security threats to Internet: a Korean multi-industry investigation", Information & Management, vol. 38, no. 8, **(2001)**, pp. 487-498.
[4] N. Z. Khidzir, A. Mohamed and N. H. Arshad, "Information Security Requirement: The Relationship between Information Asset Integrity and Availability for ICT Outsourcing", Lecture Notes on Information Theory, vol. 1, no. 3, **(2013)**, pp. 118-123.
[5] A. Marucheck, N. Greis, C. Mena and L. Cai, "Product safety and security in the global supply chain: Issues, challenges and research opportunities", Journal of Operations Management, vol. 29, no. 7-8, **(2011)**, pp. 707-720.
[6] S. Myagmar, A. J. Lee and W. Yurcik, "Threat modeling as a basis for security requirements", Symposium on Requirements Engineering for Information Security (SREIS) 2005, **(2005)** August, pp. 1-8.
[7] C. Raspotnig and A. Opdahl, "Comparing risk identification techniques for safety and security requirements", Journal of Systems and Software, vol. 86, no. 4, **(2013)**, pp. 1124-1151.
[8] E. Sikora, B. Tenbergen and K. Pohl, "Industry needs and research directions in requirements engineering for embedded systems", Requirements Engineering, vol. 17, no. 1, **(2012)**, pp. 57-78.
[9] T. Sommestad, M. Ekstedt and P. Johnson, "A probabilistic relational model for security risk analysis", Computers & Security, vol. 29, no. 6, **(2010)**, pp. 659-679.
[10] H. Suleiman and D. Svetinovic, "Evaluating the effectiveness of the security quality requirements engineering (SQUARE) method: a case study using smart grid advanced metering infrastructure", Requirements Engineering, vol. 18, no. 3, **(2012)**, pp. 1-29.
[11] C. Wolter, M. Menzel, A. Schaad, P. Miseldine and C. Meinel, "Model-driven business process security requirement specification", Journal of Systems Architecture, vol. 55, no. 4, **(2009)**, pp. 211-223.
[12] Q. Yeh and A. J. Chang, "Threats and countermeasures for information system security: A cross-industry study", Information & Management, vol. 44, no. 5, **(2007)**, pp. 480-491.

Copyright ⓒ 2014 SERSC

Copyright ⓒ 2014 SERSC