sustainability

MDPI

Article

7S Model for Technology Protection of Organizations

Hyunae Park [1], Youngcheon Yoo [1] and Hwansoo Lee [2,*]

[1] Department of IT Law, Dankook University, Yongin-si 16890, Korea; gusdo7272@naver.com (H.P.); y2c206@naver.com (Y.Y.)
[2] Department of Industrial Security, Dankook University, Yongin-si 16890, Korea
* Correspondence: hanslee992@gmail.com

Abstract: Given the importance of technologies to organizations, technology leakages can cause considerable financial losses and threaten the survival of firms. Although organizations use technology protection diagnostic models to prevent such leakages, most diagnostic models focus on cybersecurity, and the evaluation system is complex, making it difficult for SMEs to use it. This makes them unsuitable for the general technology protection diagnosis of companies. Hence, this study proposes a diagnostic model that assesses these technology protection capabilities of organizations from personnel and administrative perspectives. Drawing upon the individual elements of the 7S model—shared values, strategy, structure, systems, staff, style, and skills—our model analyzes the influence of the elements on the technology protection capabilities of organizations. To determine this influence, the study conducts a questionnaire survey among 435 employees from large, larger medium-sized, and small and medium enterprises. Using the partial least squares and the artificial neural network methods, the study determines the ranking of the relative importance of the 7s elements. The results show that the shared values element most significantly influences these capabilities. The remaining elements influence the technology protection capabilities in the following order from the greatest to the least effect: staff, strategy, structure, systems, style, and skills. These findings highlight the significance of developing an awareness of the necessity of technology protection among all the members of an organization.

Keywords: technology leakage; technology protection; 7S model; industrial security

Citation: Park, H.; Yoo, Y.; Lee, H. 7S Model for Technology Protection of Organizations. *Sustainability* **2021**, *13*, 7020. https://doi.org/10.3390/su13137020

Academic Editor: Zubair Baig

Received: 30 April 2021
Accepted: 16 June 2021
Published: 22 June 2021

1. Introduction

The leakage of technology is a grave security incident that has the potential to determine a company's future [1]. A company that seizes its competitors' technology may use the leaked information to reduce the product development costs and efforts and, in turn, cost-effectively launch a better product, thereby gaining a competitive advantage. A prominent incident of technology leakage occurred in 2003, when Cisco Systems, a manufacturer of networking equipment, filed a lawsuit accusing Huawei Technologies of copying its router software code [2]. Although Huawei reached a confidential settlement with Cisco and removed the copied source code, experts pointed out that Huawei still used Cisco's router software code. In 2003, Huawei's revenue stood at $2.1 billion, while Cisco reported a revenue of $18.8 billion. However, in 2018, Huawei earned a revenue of $92 billion, which was 87% higher than that of Cisco's $49.3 [2]. Similarly, an employee of the US company American Superconductor Corporation (AMSC) received 1.7 million dollars, an apartment, and other incentives to leak the company's turbine control software source code to China's Sinovel [3]. AMSC filed a lawsuit against Sinovel in a Chinese court and sought compensation for the financial losses from the leakage, which Sinovel refused to pay. This reduced Sinovel's stock market capitalization by half and led to a layoff of more than 60% of its employees at its headquarters. However, despite stealing AMSC's technology, Sinovel has retained its dominant position as a wind turbine manufacturer in China [3]. The aforementioned incidents demonstrate that the leakage of technology not

only weakens a company's technological competitiveness but also threatens its survival. However, companies mainly focus on investing in research associated with technological developments and often neglect investments in security measures [4]. When companies do not make sufficient budgetary allocations for security, they fail to establish the technology protection or response system required to respond to security breaches. Thus, to safeguard against or respond to technology leakages, companies should set up an efficient plan that considers which investments to prioritize for technology protection.

The technology protection diagnostic model helps a company assess the sufficiency of its security mechanisms for safeguarding its technology. By identifying and comparing insufficiently protected areas, companies can determine which security measures must be prioritized. Nevertheless, most technology protection diagnostic models are geared toward information security. The International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001 and the personal information and information security management system (ISMS-P) are the representative information security certification systems used by many companies. However, their limitation lies in the fact that their diagnostic items are skewed toward information security—they present a highly comprehensive review of content related to information security. While several academic studies have presented diagnostic models distinct from the existing information security management systems, they are characterized by a specific focus, such as having content that is geared toward small and medium-sized enterprises (SMEs) or the leakage of information [5,6]. In other words, the existing technology protection diagnostic items either preclude or have a skewed focus toward topics such as administrative, personnel, and technical security measures, which makes the items unsuitable for the general technology protection diagnosis of companies. It must also be noted that insider threats comprise the main sources of technology leakages, and hence diagnostic models must consist of items at the personnel and administrative levels. To overcome these gaps, this study aims to develop a new model that companies can use at the personnel and administrative levels to diagnose their technology protection capabilities. This study also examines and ranks, by importance, the factors affecting a company's technology protection capabilities. As the basis for its model, the study uses the McKinsey 7S model developed by Peters and Waterman (1982)—a diagnostic model of organizational management [7].

The 7S model is used in various fields of study as it can provide a practical diagnosis of an organization. An analysis reveals that most recent studies have used the 7S model to examine the security culture of organizations. These studies applied the model to specific industries and places, such as commercial banks and airports [8,9]. The analysis also reveals a lack of studies that apply the 7S model using a systematic approach to diagnose a company's technology protection capabilities. Therefore, this study uses the 7S model to present a diagnostic model that assesses these organizational capabilities from the personnel and administrative perspectives. In other words, unlike previous studies, the technology protection diagnostic model proposed in this study is composed of items developed from the personnel and administrative perspectives, and not security systems, which can be applied to assess the technology protection abilities of companies. It also verifies the effect of the individual elements of the 7S model on a company's technology protection level. Based on the implications of the verification process, this study seeks measures that can strengthen a company's technology protection capabilities. Drawing on the elements of the 7S model, this study also identifies the factors influencing a company's technology protection capabilities and uses this assessment to present detailed security measures that must be prioritized by the company. By using the diagnostic model presented in this study, companies can diagnose their technology protection capabilities and, consequently, improve the efficiency of their security-related investments and prevent technology leakages.

2. Related Research

2.1. Cases of Technology Leakages

Technology is the application of theories to a particular field or the application of procedures, methods, and knowledge to complete a task. It can be said that a company's technology reflects its competitive advantage [10]. In other words, a company that possesses useful technology with an economic value has a competitive advantage in the market [11]. In this context, Eisenhardt (1989) asserted that intense competition among companies sometimes leads to an information war [12]. Some companies use underhanded means to obtain leaked information and technology from their competitors. According to the data released by the Korean National Police Agency (2019), there were 90 to 100 annual cases of industrial espionage in South Korea, from 2015 to 2019, and 121 cases of foreign industrial espionage in the same period, and more than 300 people are implicated annually [13]. The data also reported that the police had investigated 90 cases of industrial espionage and apprehended 310 people in relation to the cases between April and October 2019; of these, 88.9% (80 cases) were classified as domestic leaks, and 11.1% (10 cases) were classified as foreign leaks. Of the enterprises that had been affected, SMEs made up 94.4% (85 cases) of the total cases, which was 17 times higher than the number of large enterprises (5.6%; 5 cases) that had been affected by the leakages. While 66.7% (60 cases) of the leaks have been attributed to insider threats, the remaining 33.3% (30 cases) have been attributed to outsider threats [13].

As demonstrated by the data, there has been a steady occurrence of leakages, both domestically in South Korea and internationally. A closer examination shows that most of these technology leakages were caused by company personnel, such as former employees, current employees, and suppliers. Of the cases in Table 1, former employees were responsible for eight of the cases, making them the most common source of leaks on the list, while three cases were attributed to current employees and the employees of suppliers. In these cases, while the former employees had taken key technical data when they resigned from their company to join a competitor or set up a competing business, the current employees had abused their authority to transfer such data to their competitors in exchange for personal gain. The employees of suppliers used the designs they received from the parent company to copy, reproduce, and supply products to the company's competitors.

Table 1. South Korean and International Cases of Technology Leakages.

Year	Case Name	Source of Leak	Detailed Description
2010	Leakage of confidential information related to Boeing's Space Shuttle program and the Delta IV rocket	Former employee	A former Rockwell and Boeing engineer sent trade secrets comprising information related to the Space Shuttle program and the Delta IV rocket to China via Chinese spies
2011	Leakage of stealth missile exhaust designs and military-technical data	Current employee	Noshir Gowadia, an engineer with the Northrop Grumman Corporation, leaked stealth missile exhaust designs and military-technical data to assist China with its cruise missile system
2015	Leakage of technology related to the insulation of cryogenic and liquefied natural gas (LNG) systems	Former employee	A former researcher from the shipbuilding industry renamed 15 files containing key technical data as "research preparation" and emailed to a Germany-based chemical company from a personal account, before moving to the company
2016	Leakage of designs related to Hyundai Heavy Industries' engine power plant	Supplier's Employee	An employee of Hyundai Heavy Industries' supplier stored designs instead of destroying them after testing parts belonging to the engine power plant. Subsequently, the supplier copied, produced, and sold the fuel injection system to distributors and other parties.

Table 1. *Cont.*

Year	Case Name	Source of Leak	Detailed Description
2017	Leakage of designs related to membrane tanks for LNG storage	Former employee	A former team leader of a research institute had stolen the designs of membrane tanks developed by the institute. After resigning from the institute, this ex-employee joined a new company and used the stolen designs to construct a new factory and build mold manufacturing facilities for membrane tanks
2017	Leakage of technology related to Waymo's LiDAR	Former employee	Anthony Levandowski illegally obtained R&D information while employed at Waymo, an R&D company specializing in autonomous driving technology. After resigning, he joined a new company, Otto, and used the technology.
2018	Leakage of technology related to Samsung Display's edge display	Supplier's Employee	TOPTEC, a manufacturer of Samsung Display, was exclusively supplying products to Samsung and was also under the confidentiality agreement. However, TOPTEC leaked the technology behind the products to a Chinese company in exchange for financial gain
2019	Leakage of wet etching techniques for displays	Former employee	Upon resignation, a former developer of a South Korean SME transferred the entire technology-related source code of its company to a USB. A Chinese company that subsequently hired the developer used this leaked information.
2019	Leakage of BASF's confidential information related to semiconductors	Former and current employees	The former and current employees of BASF leaked manufacturing-related technologies to China
2020	Leakage of key technology related to autonomous vehicles	Current employee	A professor at the Korea Advanced Institute of Science and Technology (KAIST) signed a research service contract with the Chongqing University of Technology in China without notifying KAIST. Subsequently, the professor leaked KAIST's research data on the light detection and ranging technology of the autonomous vehicles to the researchers of the Chinese university
2020	Leakage of technology belonging to the Agency for Defense Development (ADD)	Former employee	More than 20 retired ADD researchers leaked a considerable amount of data on weapons-related technologies and information over the course of years
2020	Leakage of SoftBank's confidential information	Former employee	A former employee used an office computer to access the company's server and steal confidential manuals. Subsequently, the employee allowed a Russian trade diplomat to take pictures of the office computer screen containing confidential information and to encode the photo data
2020	Leakage of Samsung's supplier SK Hynix's semiconductor technology	Supplier's Employee	The supplier company SK Hynix leaked core technologies to a competing Chinese semiconductor company

As shown in Table 1, most cases of technology leakage are caused by the personnel leaving a company. The loss of human resources occurs all around the world. In this context, it must be noted that, in recent years, companies and countries around the world have been competing to recruit highly skilled talent. This is because skilled talent significantly contributes toward furthering existing technologies and thereby stimulates the development of key future technologies [14]. However, companies focus on investments

in research for building technological resources while neglecting similar investments for retaining skilled human resources [4]. The recruitment of skilled human resources may positively impact the competitiveness of an industry, in particular, and a country, in general. Therefore, companies must be committed to protecting their technology at the personnel level, to retain their skilled human resources.

2.2. Technology Protection Models

To prevent technology leakage, countries have set up technology protection guidelines. For instance, Korea's representative guidelines are the manual for trade secret management, industrial technology protection guidelines, and technology protection guidelines for small and medium-sized enterprises [15–17]. Similar technology protection guidelines have also been established in countries such as the United States, Hong Kong, and Australia by the National Institute of Standards and Technology, the Office of the Government Chief Information Officer, and the Australian Cyber Security Center, respectively. These guidelines are a security self-assessment guide for information technology systems (SP800-26—the United States), a practice guide for security risk assessment and audit (ISPG-SM01—Hong Kong), and the Australian government's information security manual (ISM—Australia) [18–20]. Table 2 shows the technology protection framework of South Korea and other countries.

Table 2. Framework of Technology Protection.

Classification		Evaluation Area	Evaluation Item
South Korea	The Manual for Trade Secret Management	Managerial Security	Trade Secret Policies Trade Secret Classification Trade Secret Management
		Personnel Security	Personnel Security Partners Management Planning of Security Education
		Physical Security	Documentation Security Control Area Designation Computer Management
	Industrial Technology Protection Guidelines	Managerial Security	NDA: NON-DISCLOSURE AGREEMENT Security Policies Incident Response
		Personnel Security	Appointment of Professionals Professionals Classification Education and Training for Professionals
		Physical Security	Protection Area Management Baggage Inspection
		Technical Security	Protection Area Security Information Asset Management
	Technology Protection Guidelines for Small and Medium-Sized Enterprises	Policies of Technology Protection	Appointment of Technical Protection Department Asset Management
		Personnel Security	Personnel Management NDA: NON-DISCLOSURE AGREEMENT Employees' Invention System
		Facilities Management	Appointment of Protection Area Protection Facilities Area-specific Security Management
		Information System Management	Periodically Backup Unnecessary System Uninstall Security Program Installation

Table 2. *Cont.*

Classification			Evaluation Area	Evaluation Item
Other Countries	U.S. (NIST)	Security self-assessment guide for information technology systems (SP800-26)	Management Controls	Risk Management Review of Security Controls Life Cycle Authorize Processing System Security Plan
			Operational Controls	Personnel Security Physical Security Production, Input/Output Controls Technical Security
			Technical Controls	Identification and Authentication Logical Access Controls Audit Trails
	Hong Kong (OGCIO)	Practice guide for security risk assessment & audit (ISPG-SM01)	IT Security Policies	Security policy is well documented and easy to understand All rules stated in the security policy are implemented
			Human Resource Security	All staff are advised with acknowledgment of their IT security responsibilities All roles & responsibilities are clearly defined
			Asset Management	Information is properly classified and its storage media is labeled and handled according to Security Regulations
			Access Control	Each user is given with unique user identity User are informed about their privileges and access rights
			Physical and Environmental Security	UPS are installed for necessary equipment Smoking, food, and drinks are not allowed inside the computer room
			Technical Security	Network Management Firewall Management
	Australian (ACSC)	Australian Government Information Security Manual	Security documentation	Development and management of documentation System-specific documentation
			Personnel Security	Cybersecurity awareness-raising and training Access to systems and their resources
			Physical Security	Facilities and systems ICT equipment and media

The South Korean guidelines related to technology protection can be largely divided into four areas—administrative, physical, technical, and personnel security measures. Administrative security focuses on the establishment of a technology protection model, such as enacting security management regulations and setting up security strategies. Physical security is concerned with the establishment of protected areas and the management of facilities and systems, while technical security deals with the management of access rights and security technologies, among others. Finally, personnel security informs the organization's personnel about their obligations, role, and responsibilities toward technology protection by carrying out security training activities.

Overall, the South Korean and international guidelines include most of the factors that must be considered when diagnosing a company's security capabilities. However, as South Korean guidelines regarding technology protection focus on specific types of technology, it may not be suitable to use them to diagnose the technology protection capabilities of all companies. The manual for trade secret management focuses on trade

secrets, the industrial technology protection guidelines deal with industrial technology, and the technology protection guidelines for small and medium-sized enterprises focus on the technologies used by the SMEs. Therefore, an SME with trade secrets may face a dilemma when choosing the right guidelines to diagnose its technology protection capabilities. The international guidelines related to technology protection also tend to focus on specific areas. The SP800-26 deals with information technology systems, the ISPG-SM01 focuses on the assessment of security risks, and ISM addresses the diagnostic items that focus on information security.

The most representative diagnostic models for technology protection are ISO/IEC 27001 and ISMS-P (see Table 3). The ISO/IEC 27001 is an international standard for information security management systems; it defines the standards that an organization must follow to manage its information security and regulates the requirements needed to conduct the documentation of information security management systems [21]. The ISMS-P of the Korea Internet and Security Agency (KISA) is an integrated certification system that combines the ISMS (an information security management system) and the PIMS (a personal information management system) and consists of 102 certification standards [22]. Although the ISMS-P and ISO/IEC 27001 are information security management systems, some of their content also pertains to administrative, physical, and personnel security measures. However, as the content of the control items is comprehensive and focuses on information security, the above systems are considered unsuitable for diagnosing the technology protection capabilities of individual companies.

Table 3. Evaluation Model for Technology Protection.

Evaluation Area		Evaluation Item
ISO/IEC 27001	Managerial Security	Information security policies Operations security Organization of information security Human resource security Asset management Supplier relationships Information security incident management Information security aspects of business continuity management Compliance; with internal requirements, such as policies, and with external requirements, such as laws
	Physical Security	Physical Security Environmental Security
	Technical Security	Cryptography Operations security Communications security System acquisition, development, and maintenance
ISMS-P	Managerial security system	Managerial security system Risk Management Managerial Security System development and maintenance
	Protection Plan	Policies, Organizational and Asset management Human Resource Security Outsider Security Physical Security Access Control Cryptography System Development Security System Operations security Incident Response
	Personal Information Management System	Protection System for Personal Information

To solve this problem, several studies have attempted to develop a comprehensive technology protection diagnostic model that includes personnel and administrative security measures. Table 4 lists the existing research on the technology protection diagnostic model. For instance, Johansson and Johnson (2005) presented the enterprise information security cube (EISC). Chang (2010) developed a diagnostic model for the prevention of industrial technology leakage for SMEs [5,23]. Bae et al. (2016) revised and supplemented the K-ISMS to construct a set of evaluation items related to industrial security that could assess security certification systems in all the industries [24]. Currently, Kim et al. (2020) presented a security assessment diagnostic model emphasizing the prevention of information leaks from the perspective of insider threats [6]. Previous studies have discussed various ways to diagnose and improve a company's technology leakage and suggested a novel diagnostic model suitable for the company's characteristics or environment. While it is easy to manage the detailed elements of technology leakage due to the specificity of the diagnostic index, it is difficult for the average company to utilize such a model due to the complexity of the diagnostic system. Moreover, existing diagnostic systems have been developed with a focus on information security, and SMEs with a relatively low level of security system find it difficult to adopt them.

S Model for Technology Protection

As demonstrated above, the existing diagnostic models comprise diagnostic items that mainly focus on information security or companies in a specific industry. Although a few studies have presented diagnostic models including content on personnel and administrative security measures, these models have remained at the conceptual level. Thus, there is a lack of technology protection diagnostic models that can be comprehensively applied to companies in general.

The technology protection diagnosis of a company must be structured so that it can be applied to companies at the personnel and administrative levels. This is because technology leakages may occur intentionally or unintentionally by technology developers [25]. In fact, 64.5% of technology leakages were found to be caused by insider threats. Insiders have easy access to an organization's assets and confidential information, and hence they may intentionally pose a greater threat to the organization than that of the outsiders [26,27]. Moreover, if an organization does not share information related to technology protection, insiders may unintentionally leak confidential information in the process of sharing information [27]. Therefore, companies should conduct technology protection activities focusing on their human resources at the administrative level.

Table 4. Research on the Evaluation Model for Technology Protection.

Authors	Evaluation Area	Evaluation Item
Johansson and Johnson [23]	Scope	Technical, Organizational, Environmental
	Purpose	Responsive, Detective, Preventive
	Time	Planning, Operating, Controlling
Chang [5]	Investment Accounts for Technology Protection	Technology Protection Education and Training
	Environment of Industrial Technology Protection	Managerial Security Human Resource Security
	Structure of Industrial Technology Protection	Physical Security Technical Security

Table 4. *Cont.*

Authors	Evaluation Area	Evaluation Item
Bae, Kim, and Chang [24]	Environment of Industrial Technology Protection	Industrial Security Investment accounts Knowledge for Employees of Regulations about Industrial Technology Protection Related Business
	Information Security Policies	Review of Policy and Management of Policy Document Effectiveness Assessment of Regulations about Industrial Technology Protection
	Organization of Information Security	Appointment of Chief Information Security Officer Information Security Committee
	Outsider Security	Execution Management of Outsider Security Security after Outsider Contract
	Industrial Asset management	Identification of Information Asset Intellectual Property Right Management
	Industrial Security Education and Training	Planning of Education Execution Assessment of Education Program
	Human Resource Security	Appointment of Main Person in Charge Foreign Employee Management and Outsourcing Employee and Visitor Management
	Physical Security	Appointment of Protection Area Protection Facilities Mobile Security
	System Development Security	Definition of Security Requirement Security Log
	Cryptography	Cryptography Policies
	Access Control	Establishment of Access Control Policy User Registration and Authorization
	Operation Management	Operational Procedure and Responsibilities Acquisition of Information System
	Incident Response to Industrial Technology Protection	Experience of leakage Number and cost of technology leakage
	Emergency Accident Management	Response Plan and System Digital Forensic
	IT Disaster Recovery	Establishment of IT Disaster Recovery System
	Difficulties and Policy Recommendations of Industrial Technology Protection	Application in Operation of Information Instrument Technology Leakage Risk Assessment Assessment of Management Level
Kim, Lee, and Chang [6]	Security change management	Measuring and improving the security level
		Incident response
	Security operation management	Physical security system Electronic security system Managerial security system Classification of developed technology
	Security support environment	Security organization and investment
	Security culture	Internal/External security culture

This study used the 7S model to develop a general technology protection diagnostic model covering the personnel and administrative perspectives. Several studies have

used the 7S diagnostic model because it focuses on organizational management, and the elements of its strategic process may be used to perform a concise and practical diagnosis of an organization. The model includes seven elements—shared values, strategy, structure, systems, staff, style, and skills. Although it has been primarily used in the field of business administration, its scope has expanded in recent years and the model is now widely used in the field of security [7,8].

Previous studies applying the 7S model in the field of security have primarily discussed the security and organizational culture of specific types of companies. Lim (2017) utilized the 7S and competing values models to develop a tool that diagnoses the security and organizational culture of companies, while Chen and Liu (2010) used the 7S model to present an operational risk management framework for commercial banks [8,28]. Gechkova and Kaleeva (2020) applied the 7S model to airports and proposed a plan to improve their security systems and thereby prevent technology leakages [9]. As demonstrated above, existing studies mainly present a model that diagnoses a company's technology protection capabilities from the perspective of a specific industry or type of company. Accordingly, there have been few studies on technology protection diagnostic models that can be applied to companies in general. Since technology leakage is related to various factors such as strategy, personnel management, organizational structure, and security awareness in addition to security system vulnerabilities, it is necessary to undertake an academic discussion of technology leakage diagnosis from a comprehensive perspective.

The 7S model can also be applied for the technology protection of companies. The fact that the whole organization shares the importance and value of protecting its technology, which is included as a management goal, may correspond with the 7S model's element of shared values. In this context, Von Solms (2006) stated that an organization must have a security culture and that its personnel must understand the importance of technology protection for technology protection activities to take effect [29]. To achieve this, Von Solms (2006) argued that an organization must support its personnel so that it acquires the necessary knowledge and skills regarding technology protection [29]. An organization can also minimize the risks posed to its assets by having a systematically established security culture. In this regard, it must be understood that it would not be possible to conduct meaningful technology protection activities if only some, and not all, of the organization's personnel or members of the management team, possess an awareness of the importance of protecting its technology. In other words, technology protection activities cannot be conducted if the entire organization does not have shared values regarding technology protection.

This study developed a technology protection model based on the 7S model (see Table 5). The strategy element of the 7S model corresponds to the establishment of a company technology protection strategy and other related measures. Sullivant (2016) argued that a company can give strategic priority to technology protection activities and allocate a sufficient budget to implement this strategy [30]. The author also asserted that an appropriate response and recovery strategy is necessary to protect a company's technology, as the use of a one-time prevention and detection diagnostic model cannot guarantee complete security.

The structural element of the 7S model is related to an organization having a systematic organizational structure for technology protection and having a manager in charge of the technology protection division and security for the efficient operation and management of security-related responsibilities. Bacal (2004) argued that it may be difficult to carry out security management activities when an organization is not designed or structured systematically and that a disorganized organization may face difficulties when making decisions related to its technology protection activities [31].

The system elements of the 7S model correspond to an organization's maintenance of the regulations relevant to protecting its technology and to the organization's control and monitoring of its technical data. In this context, it must be noted that when an organization's personnel is provided with benefits such as pay raises, welfare benefits, and

other incentives, it may feel a greater sense of responsibility toward the organization and deliver increased productivity [32]. Therefore, the establishment of a technology protection model is related to the protection of an organization's technology.

Table 5. 7S model for technology protection.

Classification	Definition
Shared Values	The content on the importance of technology protection is integrated with a company's shared goals and core values.
Strategy	An established technology protection strategy and sufficient budgetary allocation for the strategy
Structure	The way a company is organized to protect its technology
Systems	The activities and procedures necessary for technology protection
Staff	Members' understanding of roles and responsibilities toward technology protection
Style	The management team's perception of technology protection
Skills	The skills of employees in charge of technology protection and the competency of those skills

The staff element of the 7S model corresponds to the personnel's understanding of their role and responsibilities toward protecting the organization's technology and their adherence to the relevant regulations and directives. In this regard, AlHogail and Mirza (2014) asserted that to prevent technology leakage, an organization's personnel must be educated about technology protection so that they understand their role and responsibilities toward technology protection [33]. The study showed that humans are more responsible than the technical factors for the technology leakages. Therefore, the study argued the importance of improving the personnel's attitude and awareness toward technology protection.

The leadership style element of the 7S model refers to a management team's interest in technology protection. A management team can significantly impact an organization and its personnel and contribute toward the development of an organizational culture. Accordingly, if a management team is indifferent to the issue of technology protection, it would be impossible to generate active internal support for the organization's efforts to protect its technology [34]. Moreover, as the protection of technology does not generate direct revenue, it may be difficult to pursue technology protection activities without management's consideration.

The skills element of the 7S model is related to how an organization can enhance the technology protection expertise of its personnel. This can be achieved when the personnel responsible for their organization's technology protection obtain professional certifications or receive professional training in technology protection. Ravanfar (2015) highlighted the need to possess professional skills to protect technology, given the constant development of new technologies and technological advancements [35]. Hence, the study argued that relevant personnel must receive regular professional training in technology protection.

3. Research Model and Hypothesis Development

This study developed a research model to analyze which elements of the 7S model significantly impact the technology protection capabilities of an organization. It performed an empirical analysis after establishing the hypotheses that all seven elements—shared values, strategy, structure, systems, staff, style, and skills—influence the technology protection capabilities of organizations. A control variable for company size was also added to the research model (Figure 1).

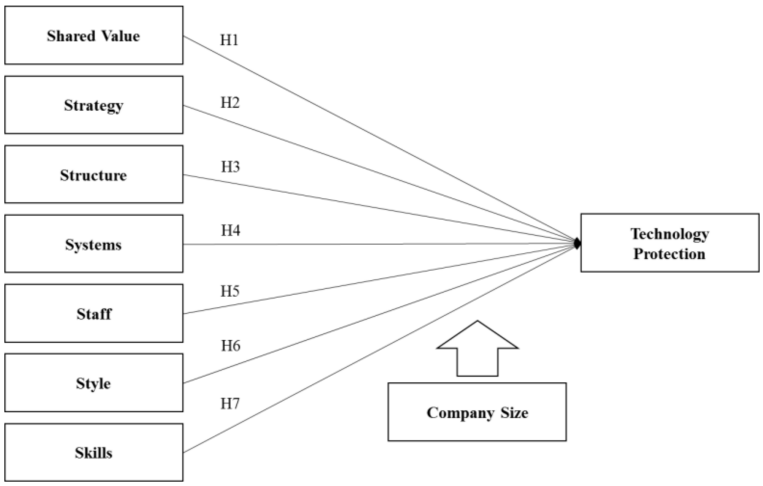

Figure 1. Research Model.

Von Solms (2016) asserted that the risk of technology leakages reduces when an organization's personnel holds common technology protection goals and works in cooperation with the organization. The study also argued that an organization's investment in technology protection is reduced when there is internal cooperation on issues concerning technology protection [29]. This is because such cooperation increases an organization's problem-solving ability and improves its decision-making processes. Conversely, when there is a lack of internal cooperation and information sharing, there is a greater likelihood of personnel to leak confidential information intentionally or unintentionally. This is because inaccurate or distorted information can cause commotion in the organization [27]. An organization and its personnel must share a common value and the importance of protecting its technology. It must be noted that leakages occur even when a systematic strategy, organizational structure, and a technology protection model are put in place to protect technology. This is because the lack of an organizational culture that shares the value of technology protection could lead to the propagation of inaccurate and distorted information within the organization.

Hypothesis 1 (H1): *The shared value element will have a positive (+) effect on the technology protection capabilities of an organization.*

A strategy is a plan or direction taken to operate an organization smoothly. Anderson and Choobineh (2008) asserted that the absence of a strategy may lead to the implementation of technology protection activities with insufficient or nonexistent resources [36]. Given this, the study argued that an organization can minimize the risk of technology leakages and provide a swift response if they occur by establishing a strategy for technology protection in advance. As technology protection activities are neither temporary nor carried out for a short period, Sullivant (2016) stated that it is advisable to prepare a relevant plan for implementing the technology protection activities in a systematic manner [30]. The study also indicated that an organization can be strengthened by establishing a strategy for technology.

Hypothesis 2 (H2): *The strategy element will have a positive (+) effect on the technology protection capabilities of an organization.*

Modenov and Vlasov (2018) asserted that the existence of a systematic organizational structure and a division in charge of protecting an organization's technology may influence the organization's technology protection capabilities [37]. Even with a systematic strategy, it would be difficult to conduct technology protection activities in the absence of a functional department to manage and operate such activities. It must be noted that

most SMEs do not have a division to carry out technology protection activities; in the cases when there is a division, the general affairs department often treats it as a division in charge of incidental responsibilities or those related to technology protection and other responsibilities. This approach may adversely affect a division's expertise in technology protection. Therefore, companies must set up a division with a manager to oversees their technology protection responsibilities.

Hypothesis 3 (H3): *The structural element will have a positive (+) effect on the technology protection capabilities of an organization.*

Antoni et al. (2017) stated that most cases of technology leakages are related to monetary gain or other personal benefits and that some companies set up the relevant regulations and operate a reward and punishment system to prevent their occurrence [38]. However, it argued that the penalties for committing technology leakages are too lenient; it also showed the existence of inadequate compensation systems for technical personnel. Several companies lack the relevant regulations and a reward and punishment system. Therefore, companies must establish relevant regulations and use harsher penalties for leakages while providing more practical benefits to their technical personnel. Naipinit et al. (2014) asserted that the provision of benefits may motivate personnel to protect the organization's technology, and thereby positively impact a company's technology protection capabilities [32].

Hypothesis 4 (H4): *The existence of a system will have a positive (+) effect on the technology protection capabilities of an organization.*

Furnell and Clarke (2005) asserted that a company's security culture can be determined by the behaviors and abilities of its personnel [39]. Thus, if an organization comprises members who are uncooperative on matters pertaining to technology protection activities, the activities may lose their effectiveness even if the organization implements strict regulations and a systematic strategy. Conversely, if all personnel have a positive perception of the technology protection activities, they would understand their role and responsibilities in protecting their organization's technology and faithfully adhere to security regulations, such as by observing the relevant regulations and directives [33]. Therefore, when an organization's personnel have a positive perception of security-related issues, it can significantly impact the organization's technology protection capabilities.

Hypothesis 5 (H5): *The staff element will have a positive (+) effect on the technology protection capabilities of an organization.*

Singh (2013) argued that technology leakages are usually evaded; given that such incidents do not develop into social issues, the management team of an organization overlooks the importance of security management activities [34]. In particular, it was pointed out that SMEs often neglect their technology protection activities because they only focus on producing tangible results for financial reasons. When a company's CEO is indifferent to the issue of technology protection, it may lead to an inadequate security management system and ultimately cause a technology leakage. A transformational leader influences the entire organization [40]. In other words, the technology protection activities of an organization can change according to the leadership style of its CEO.

Hypothesis 6 (H6): *The style element will have a positive (+) effect on the technology protection capabilities of an organization.*

With the outbreak of the COVID-19 pandemic, many companies have adopted telecommuting practices, which increase the risk of technology leakage. This is because when employees work remotely, they work in an environment that is not under the direct control

of the company. Telecommute practices contribute toward increased use of USBs and external hard drives as well as the use of unsecured networks [41]. Given that societal changes are presenting new threats to the security of companies, Ravanfar (2015) argued that to prevent security breaches, the division and personnel in charge of technology protection must have a high level of understanding of new security environments and have expertise in various security technologies [35]. There will be a difference between the technology protection activities and the resulting outcomes of companies that have technology protection experts with practical experience and those that do not have such experts.

Hypothesis 7 (H7): *The skills element will have a positive (+) effect on the technology protection capabilities of an organization.*

4. Method and Data

This study surveyed to determine the effect of the 7S model's individual elements on the technology protection capabilities of an organization. The questionnaire consisted of 28 items, with 4 items for each element; the study used a 7-point Likert scale to measure the responses, ranging from 1 (strongly disagree) to 7 (strongly agree). The questionnaire items were developed by partially modifying the items of an existing organizational culture-related questionnaire to suit the subject of technology protection. The measurement items and referenced studies are listed in Table 6.

Table 6. Items for measuring the level of technology protection based on the 7S model.

Element		Items	References
Shared Values	SV1	My company shares the importance and value of technology protection.	[29]
	SV2	My company includes the concept of technology protection in its management goals.	
	SV3	My organization is aware of the necessity for technology protection.	
	SV4	My company has an organizational culture that protects its technology.	
Strategy	SG1	My company has a technology protection strategy.	[7]
	SG2	For my company, technology protection is a strategic priority.	
	SG3	My company has a technology protection plan.	
	SG4	My company invests a sufficient budget for protecting its technology.	
Structure	SU1	My company has a systematic organizational structure for protecting its technology.	[31]
	SU2	My company has a division in charge of its technology protection responsibilities.	
	SU3	My company has a manager in charge of the technology protection responsibilities.	
	SU4	My company operates and manages its technology protection responsibilities efficiently.	
Systems	SM1	My company has the relevant regulations to protect its technology.	[32]
	SM2	My company controls and monitors its technical data.	
	SM3	My company uses confidentiality and non-compete agreements to protect its technology.	
	SM4	My company uses rewards for employees who are excellent at protecting the company's technology and punishments for those who violate regulations.	
Staff	SF1	The members of my company understand their roles and responsibilities toward protecting the company's technology.	[33]
	SF2	The members of my company strictly adhere to the relevant regulations and directives to protect the company's technology.	
	SF3	The members of my company receive training related to technology protection.	
	SF4	The members of my company respect the managers in charge of technology protection.	

Table 6. *Cont.*

Element		Items	References
Style	SY1	The management team at my company has a high level of interest in technology protection.	[34]
	SY2	The management team at my company recognizes that technology protection is important to business activities.	
	SY3	The management team at my company actively supports the protection of the company's technology.	
	SY4	The management team at my company takes the issue of technology protection into account during decision-making processes.	
Skills	SK1	At my company, the division in charge of the company's technology protection has expertise in technology protection.	[35]
	SK2	At my company, the members of personnel in charge of the company's technology protection have professional certifications.	
	SK3	At my company, the division or personnel in charge of the company's technology protection receive the relevant professional training.	
	SK4	My company has a response manual for the occurrence of technology leakages.	
Technology Protection	TP1	My company protects technology-related confidentiality well.	[6]
	TP2	My company is better at managing security than are other companies.	
	TP3	My company has fewer technology leaks or security incidents compared to other companies.	
	TP4	My company has never suffered major damage from technology leaks or security incidents.	

This study conducted a survey using the Open Survey service. Open Survey is the dominant mobile survey company in the Republic of Korea [42]. In February 2021, the data were collected from the completed questionnaires of 500 office workers. Of these, 65 questionnaires were excluded, owing to multiple responses to 90% or more items. The study analyzed 435 questionnaires. Table 7 presents the demographic characteristics of the participants. Of the participants in the sample, 310 were male (71.3%) and 125 (28.7%) were female. Thus, the male participants provided a higher number of responses than the female participants. Concerning the participants' age groups, the study considered the nature of the questionnaire, which led to the exclusion of the teenage groups. The age groups of the recruited participants were evenly distributed, with 120, 108, 115, and 92 participants belonging to the age groups of 20 years (27.6%), 30 years (24.8%), 40 years (26.4%), and 50 years (21.1%), respectively. Concerning the participants' level of education, 27, 12, 323, 6, and 67 participants were high school graduates or less (6.2%), college students (2.8%), college graduates (74.3%), graduate school students (1.4%), and graduate school graduates (15.4%), respectively. Thus, college graduates made up the highest percentage in the sample. Concerning the size of the company, 125, 111, 175, 7, 8, and 9 participants worked in a large enterprise (28.7%), larger medium-sized enterprise (25.5%), an SME (40.2%), a research institute (1.6%), an educational institution (1.8%), and other places (2.1%), respectively. Employees of large enterprises, larger medium-sized enterprises, and SMEs accounted for the highest percentage of participants in the sample. With the exclusion of interns (contract workers) and executive-level employees or above, job position levels were evenly distributed. Concerning the fields of technology, 129 participants worked in the manufacturing industry (e.g., textile and processing industries) (29.7%), while 108 participants worked in a professional, science, or technical service industry (e.g., R&D industry) (24.8%).

Table 7. Demographic Characteristics.

Classification	Classification	N	%
Gender	Male	310	71.3%
	Female	125	28.7%
Age	20 years	120	27.6%
	30 years	108	24.8%
	40 years	115	26.4%
	50 years	92	21.1%
Degree	High School Graduates or Less	27	6.2%
	College Students	12	2.8%
	College Graduates	323	74.3%
	Graduate School Students	6	1.4%
	Graduate School Graduates	67	15.4%
Company Size	Large Enterprise	125	28.7%
	Larger Medium-Sized Enterprise	111	25.5%
	SME (Small and Medium-sized Enterprise)	175	40.2%
	Research Institute	7	1.6%
	Educational Institute	8	1.8%
	Other Places	9	2.1%
Job Position	Intern (Contract Worker)	6	1.4%
	Staff	112	25.7%
	Assistant Manager	94	21.6%
	Manager	91	20.9%
	Deputy General Manager	51	11.7%
	General Manager	54	12.4%
	Executives	27	6.2%
Technical Field	Manufacturing Industry (Weaving, Process Manufacturing, etc.)	129	29.7%
	Waterworks Industry	9	2.1%
	Construction Industry	21	4.8%
	Wholesale and Retail	30	6.9%
	Information Service Industry	28	6.4%
	Financial business and Industry	20	4.6%
	science, or technical service industry	108	24.8%
	Business supporting Service Industry	21	4.8%
	Public Administration Service Industry	31	7.1%
	Other Field	38	8.7%
Total (N)		435	

5. Results

5.1. Verification of the Measurement Model

To verify the research model, this study used a multi-analysis method integrating the smart PLS v2.0 (partial least squares) and the statistical package for the social sciences (SPSS) 26.0 program's artificial neural network (ANN). While partial least squares

structural equation modeling (PLS-SEM) is useful for hypothesis testing, ANN is a strong statistical technique for predicting outcome variables [43]. In particular, ANN can be applied when the interaction between the independent and dependent variables is non-linear and complex. The two-stage approach integrating PLS-SEM and ANN enables meaningful analysis by complementing the weaknesses of each methodology. This study used both methods to increase the accuracy of the research results [44]. Here, factor and element are considered the same concepts. Since the term "factor" is common in statistical analysis, the word "factor" is used instead of "element" in the analysis section.

Before verifying the research model, this study performed an exploratory factor analysis (EFA) to determine whether the questionnaire items of each variable were loaded into one factor. The varimax rotation method was used to determine the seven factors. Four items of the style factor, three items of the structure factor, four items of the strategy factor, three items of the shared values factor, three items of the skills factor, three items of the system factor, and two items of the staff factor were loaded on the first, second, third, fourth, fifth, sixth factor, and seventh factors, respectively. Six items (SU1, SV4, SK1, SM4, SF3, and SF4) were excluded from the analysis because they did not share common characteristics or had factor loadings less than or equal to 0.5 [45]. The study performed 7 rotations, and 22 items of the 7 factors were used to verify the research model. The EFA results are shown in Table 8.

Table 8. Exploratory factor analysis.

Classification		Factor 1	Factor 2	Factor 3	Factor 4	Factor 5	Factor 6	Factor 7
Style (SY)	SY1	0.812	0.178	0.279	0.143	0.086	0.073	0.135
	SY2	0.810	0.158	0.185	0.199	0.111	0.162	0.115
	SY4	0.692	0.111	0.196	0.158	0.355	0.116	0.270
	SY3	0.646	0.266	0.245	0.193	0.322	0.176	0.095
Structure (SU)	SU3	0.158	0.810	0.161	0.133	0.218	0.174	0.196
	SU2	0.195	0.793	0.233	0.135	0.235	0.148	0.109
	SU4	0.225	0.755	0.239	0.151	0.185	0.177	0.180
Strategy (SG)	SG2	0.371	0.201	0.748	0.217	0.144	0.018	0.083
	SG3	0.220	0.264	0.703	0.278	0.197	0.249	0.150
	SG4	0.312	0.304	0.650	0.132	0.215	0.205	0.152
	SG1	0.194	0.179	0.648	0.360	0.213	0.140	0.248
Shared Value (SV)	SV1	0.074	0.056	0.129	0.794	0.201	0.224	0.148
	SV2	0.241	0.168	0.308	0.749	0.052	0.070	−0.015
	SV3	0.300	0.204	0.213	0.671	−0.010	0.096	0.329
Skills (SK)	SK4	0.171	0.190	0.172	0.173	0.782	0.120	0.217
	SK2	0.337	0.415	0.214	0.019	0.637	0.092	−0.030
	SK3	0.245	0.401	0.254	0.102	0.612	0.133	0.243
Systems (SM)	SM3	0.230	0.149	0.116	0.180	0.070	0.859	0.098
	SM1	0.088	0.466	0.212	0.159	0.197	0.598	0.283
	SM2	0.104	0.406	0.259	0.215	0.232	0.542	0.403
Staff (SF)	SF1	0.254	0.289	0.189	0.195	0.197	0.223	0.712
	SF2	0.330	0.262	0.248	0.239	0.239	0.230	0.612

To verify the measurement model, we calculated the values of the average variance extracted (AVE), composite reliability, and Cronbach's alpha. Generally, the reliability and validity of a variable's measurement items are considered to be high if the values

of composite reliability and Cronbach's alpha are greater than or equal to 0.7. The data analysis results revealed that the value of composite reliability was greater than or equal to 0.88, and the value of Cronbach's alpha was greater than or equal to 0.79, for all the variables. The values satisfied the reliability and validity of the measurement items. Convergent validity is confirmed when the AVE value is greater than or equal to 0.5, and this study found that the AVE value of all the variables was greater than or equal to 0.71. Discriminant validity is satisfied when the square root value of the AVE of each variable is greater than those of other variables on the vertical and horizontal lines, and it was found that the square root value of the AVE of all the variables was greater than those of the other variables [46]. Therefore, convergent and discriminant validities were also satisfied for all variables (see Table 9).

Table 9. Reliability and Validity Assessment.

Variable	AVE	CR	C-alpha	SV	SG	SU	SM	SF	SY	SK	TP
SV	0.71	0.88	0.79	0.84							
SG	0.75	0.92	0.89	0.66	0.87						
SU	0.83	0.94	0.90	0.47	0.65	0.91					
SM	0.76	0.91	0.85	0.55	0.63	0.69	0.87				
SF	0.85	0.92	0.83	0.59	0.66	0.64	0.70	0.92			
SY	0.76	0.93	0.89	0.56	0.70	0.57	0.54	0.65	0.87		
SK	0.74	0.90	0.83	0.44	0.65	0.70	0.60	0.64	0.65	0.86	
TP	0.71	0.88	0.80	0.61	0.60	0.51	0.51	0.61	0.52	0.50	0.84

5.2. Hypotheses Testing and Relative Importance

Bootstrapping was used to analyze the path coefficient of the research model. Bootstrapping is a nonparametric technique for evaluating path coefficients and weights of external factors by analyzing standard errors for estimation. In this study, 500 resamples were input. According to the hypotheses testing results, H1, H3, and H5 were significant at $p < 0.001$, $p < 0.05$, and $p < 0.01$ respectively. Among the 7S factors, it was confirmed that shared value (SV), strategy (SG), and staff (SF) has a significant influence on technology protection (TP) [44]. Figure 2 shows the overall structural model testing results.

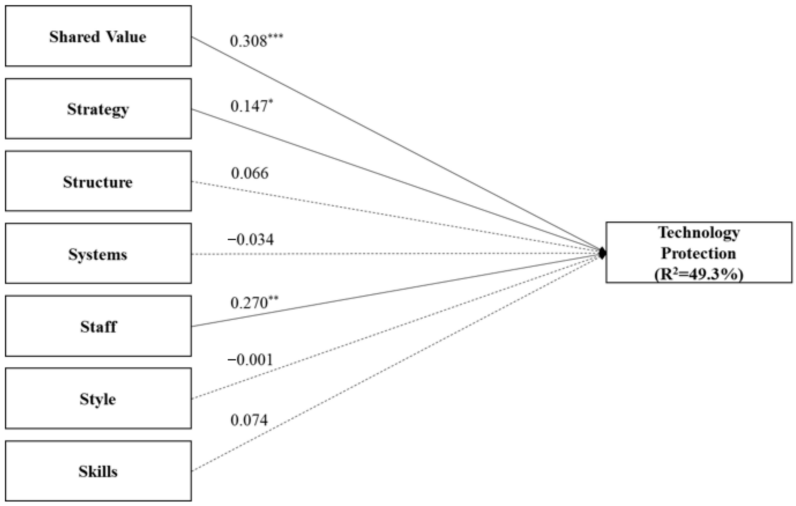

Figure 2. Hypotheses Testing Results. * $p < 0.005$, ** $p < 0.01$, *** $p < 0.001$.

Subsequently, this study examined the importance of the independent variables using the ANN multilayer perceptron. The multilayer perceptron is an effective analytical method used to identify nonlinear relationships between variables with a high prediction accuracy, and this study used the SPSS 26.0 program to perform the analysis. Before analyzing the importance of the independent variables, we split the dataset into training (90%) and testing (10%) datasets and performed cross-validation. The sigmoid activation function was used for all the input and output layers, and the root means square's (RMSE) value was calculated to increase the prediction accuracy of the analysis. The RMSE value was calculated using the following equation, which uses the sum of squared errors (SSE) and the mean squared error (MSE) values [47,48].

$$\mathrm{MSE} = \left[\frac{1}{\mathrm{N}}\right] \times \mathrm{SSE},\ \mathrm{RMSE} = \sqrt{}\mathrm{MSE} \quad (1)$$

It is considered that the lower the value of RMSE, the higher is the reliability of the results. The mean RMSE values were found to be 0.095 and 0.085 for the training (90%) and testing (10%) datasets, respectively, as a result of the ANN analysis; this confirmed the accuracy and reliability of the analysis results [49]. Table 10 shows the RMSE values for the training and testing data sets to represent an ANN model in considering the relationships between the inputs and the output.

Table 10. Artificial Neural Network (ANN) Values.

Inputs: SV, SG, SU, SM, SF, SY, SK Output: TP				
Neural Network	**Training (90%)**		**Testing (10%)**	
	SSE	**RMSE**	**SSE**	**RMSE**
ANN1	3.613	0.096	0.245	0.079
ANN2	3.529	0.095	0.323	0.086
ANN3	3.344	0.094	0.498	0.094
ANN4	3.431	0.093	0.304	0.093
ANN5	3.390	0.094	0.385	0.085
ANN6	3.649	0.097	0.324	0.085
ANN7	3.545	0.095	0.352	0.089
ANN8	3.525	0.096	0.281	0.076
ANN9	3.690	0.097	0.210	0.070
ANN10	3.630	0.096	0.334	0.095
	Mean	0.095	Mean	0.085

This study determined the average and normalized relative importance of the variables to examine the ranking of the relative importance among the independent variables (See Table 11). The results of the analysis revealed that the shared values element had the greatest effect on the technology protection capabilities of an organization. The remaining elements were found to have a positive impact on the technology protection capabilities in the following order when ranked from the greatest to the least effect: staff, strategy, structure, systems, style, and skills. Furthermore, to determine whether there is a significant difference in the effect of the above elements according to the company's size, this study grouped the large enterprises (LE) and larger medium-sized enterprises (LME) into Group A and the SMEs into Group B, before performing additional analyses. For the companies in Group A, the analysis revealed that the ranking of relative importance for the elements was as follows, from the greatest to the least effect: shared values, staff, and skills. Unlike

the companies in Group A, the staff, strategy, and structure elements ranked higher for the companies in Group B.

Table 11. Normalized Variable Relative Importance.

Classification	All			Group A (LE, LME)			Group B (SME)		
Variable	ARI	NRI (%)	Ranking	ARI	NRI (%)	Ranking	ARI	NRI (%)	Ranking
SV	0.337	100.0%	1	0.297	100.0%	1	0.137	55.5%	4
SG	0.196	58.1%	3	0.158	53.3%	4	0.176	71.4%	2
SU	0.113	33.5%	4	0.049	16.6%	6	0.164	66.5%	3
SM	0.110	32.5%	5	0.030	10.1%	7	0.100	40.3%	7
SF	0.281	83.3%	2	0.227	76.3%	2	0.247	100.0%	1
SY	0.052	15.3%	6	0.063	21.1%	5	0.126	51.2%	5
SK	0.047	14.0%	7	0.175	59.0%	3	0.113	45.6%	6

To verify the variables accurately, this study performed a comparative analysis of the results obtained using the PLS-SEM and ANN analyses. Table 12 shows the comparative analysis results. The rankings resulting from the PLS-SEM and ANN analyses were determined according to the path coefficients and normalized relative importance (%), respectively. As the ANN analysis calculates all of the linear and complex nonlinear relationships between predictor variables with a higher accuracy, the rankings of the PLS-SEM and ANN analyses may not be in complete agreement [49]. Of the independent variables, this study showed that the systems, style, and skills elements were not consistent between the two rankings, but that the top four elements were in agreement in the ranking of relative importance.

Table 12. PLS-SEM and ANN Analysis Comparison.

	Path	Path Coefficient	Finding	PLS-SEM Ranking	Normalized Relative Importance (%)	ANN Ranking	Matched
H1	SV → TP	0.308	Positive	1	100.0%	1	O
H2	SG → TP	0.147	Positive	3	58.1%	3	O
H3	SU → TP	0.066	Negative	4	33.5%	4	O
H4	SM → TP	−0.034	Negative	6	32.5%	5	X
H5	SF → TP	0.270	Positive	2	83.3%	2	O
H6	SY → TP	−0.001	Negative	7	15.3%	6	X
H7	SK → TP	0.074	Negative	5	14.0%	7	X

6. Conclusions

Given that technological leakages not only weaken a company's technological competitiveness but also its survival, companies must be active in their technology protection efforts. Specifically, they must use proactive prevention measures and provide appropriate responses to technology leakages. However, since a limited budget is allocated for a company's technology protection, the size of the investment must be considered to plan efficient investments [50]. In such circumstances, a tool allowing companies to self-diagnose their technology protection activities can improve the efficiency and effectiveness of the companies' technology protection-related investments. In other words, by diagnosing their technology protection capabilities, companies can identify the detailed technology protection-related items that they must prioritize and promote. However, existing technology protection diagnostic models focus on information security; hence, they are considered unsuitable for diagnosing the overall technology protection capabilities of companies in

specific industries. Therefore, this study used the 7S diagnostic model, which diagnoses issues at the personnel and administrative levels, to examine the elements that affect an organization's technology protection capabilities and to rank the importance of these elements. In addition, this study's model is different from existing models in that it includes the shared values factor. Even if the security policies or security systems emphasized by existing diagnostic tools are well established, security incidents can occur due to employees who do not follow or avoid them. In any case, preventing this exceptional security incident is not easy. However, if the importance of technology protection is linked to corporate strategy and its value shared with employees, a company can reduce the possibility of security incidents caused by employee deviance.

This study established the hypotheses that all the individual elements of the 7S model influence the technology protection capabilities of an organization. This study verified the research model. Specifically, through the results of both the PLS-SEM and ANN analyses, the study showed that the shared values and staff elements rank first and second, respectively, in the order of relative importance. In an organization, one of the challenges faced by security managers is the conflict of values that arise between them and the personnel concerning the technology protection activities. The conflict of values occurs when members of the personnel bypass security measures to work more efficiently and security managers work to control such occurrences. Such a conflict of values may have a negative impact on the technology protection activities of an organization. In this context, it must be noted that, even if an organization has a systematic technology protection division and a high-level security system, the effects of the organization's technology protection efforts cannot be maximized unless the entire organization is aware of the importance of technology protection. The staff element was also ranked relatively high because of its relationship with the conflict of values that may occur within an organization. This is because the personnel's negative perception of their organization's technology protection activities may lead to a lack of respect for the security manager or cause members of the personnel to violate the relevant regulations and directives. Therefore, companies must develop an innovative security culture to resolve such conflicts of value. A potential solution would be to develop a pleasant and effortless security culture by narrowing the gap between the security manager and employees and by making security more accessible to them [51].

This study found that the systems, style, and skills elements had a relatively insignificant effect on the technology protection capabilities of an organization. Companies generally tend to focus on establishing a system that allows them to control their personnel. However, a system that does not consider the necessary social and organizational factors may have a negative impact on the willingness of personnel to adhere to security measures. This demonstrates that the existence of a technology protection-related system does not necessarily lead to the security compliance behavior of an organization's personnel [52]. Concerning the style element, its relative importance may have been low because changes in corporate governance weaken the decision-making power of CEOs. Concerning the skills element, its effect on technology protection was not significant for the entire sample of companies. However, it was found to influence the technology protection capabilities of companies with a specific size. This may mean that large enterprises and larger medium-sized enterprises recognize the need for specialized security technologies because they possess relatively more competitive technologies [53].

This study also determined the independent variables' ranking of relative importance, according to the size of the companies. Ultimately, it was revealed that the shared values, staff, and skills elements influence the technology protection capabilities of large enterprises and larger medium-sized enterprises, with the elements listed in the order of the greatest to the least effect. For SMEs, the staff, strategy, and structure elements had the most significant effect, with the elements ranked from the greatest to the least effect. The study showed that the staff element ranked high in relative importance, concerning the technology protection of large enterprises, larger medium-sized enterprises, and SMEs.

However, the shared values and skills elements ranked high for large enterprises and larger medium-sized enterprises, while the strategy and structure elements ranked high for SMEs. The shared values element may have ranked high for the large enterprises and larger medium-sized enterprises because such enterprises have a greater number of departments and employees than those of the SMEs. This aspect demonstrates the significance of the awareness of the necessity of technology protection among all the employees of the organization. Given that these enterprises possess a higher number of competitive technologies, they may better recognize the need for advanced security technologies to protect their technology. Therefore, large enterprises and larger medium-sized enterprises must include technology protection in their management goals and develop an organizational culture in which the importance and value of technology protection are recognized by the entire organization. Furthermore, the division or personnel in charge of an organization's technology protection responsibilities must be provided the support that enables them to receive regular professional training and obtain relevant certifications.

In the case of SMEs, they neither have technology protection strategies nor have a relevant division to manage these responsibilities. The strategy and structure elements may have ranked high in relative importance for SMEs as a result of these characteristics. Therefore, SMEs must first design a system designed that protects their technology. To achieve this, SMEs can use the security guidelines issued by the government. Furthermore, as SMEs have a relatively low budget to invest in the security of their company, they can apply for government support programs providing technology protection-related support in the form of specialized services.

The academic significance of this study lies in its academic and practical contributions. First, it must be noted that the existing technology protection diagnostic models are either excessively comprehensive or focused on information security. Thus, these diagnostic models have a limitation in that they are not suitable for diagnosing the overall technology protection capabilities of an organization. Given this gap, the first academic contribution of this study lies in its empirical analysis of the factors affecting the technology protection capabilities of an organization. Furthermore, this study sought measures to improve an organization's technology protection capabilities. Second, this study used the 7S model to develop a technology protection diagnostic model that includes personnel and administrative perspectives. While existing technology protection diagnostic models consist of diagnostic items focusing on the issue of information security or specific types of companies, the diagnostic model presented in this study could be used to diagnose the overall technology protection capabilities of companies at the personnel and administrative levels.

As a practical contribution, this study introduces a universal assessment model for companies' technology protection. The model proposed in this study is relatively simple and easy to interpret compared to existing models; it is suitable for use as a preliminary or continuous diagnostic tool in large enterprises or in cases where it is difficult to apply the existing diagnostic model, such as in SMEs. The second practical contribution of this study lies in its ranking of technology protection activities; this ranking can help companies prioritize their technology protection goals. One characteristic of the technology protection-related responsibilities is that it is difficult to measure their performance. Hence, companies regard such responsibilities as unimportant and, as a result, do not adequately invest in their company's technology protection. In such circumstances, companies seek to gain useful returns on their security investments. If companies were to use the findings of this study to identify the technology protection activities that their company must prioritize, they would be able to carry out their technology protection responsibilities more efficiently. Third, this study determined the relative importance of the 7S model's individual elements according to the company size. By grouping large enterprises and larger medium-sized enterprises into one group and by comparing this group with that comprising SMEs, this study determined the relative importance of the seven elements and thereby proposed specific methods to improve the technology protection capabilities of an organization.

Despite these contributions, this study has a few limitations. First, the survey was conducted with general employees, not security experts. Hence, the accuracy of the diagnosis may be low since general employees have a relatively low understanding of security systems and measures. However, even for security experts, the assessment may be subjective due to work relevance and prejudice; therefore, an evaluation of the various factors resulting from security work may be more appropriately obtained from general staff evaluation. Accordingly, it would be meaningful to conduct additional research on the difference in perceptions between these two groups. Second, there is a difference in the sample size according to gender, position, and company size. Analysis based on different demographic factors can provide more insight for practice; thus, future studies need to consider the sample balance to conduct a comparative study. In particular, the differences in security awareness according to job position can contribute to the understanding of shared security value, which is a key element of this study. Finally, although this study has developed a model that can diagnose the technology protection capabilities of an organization from an administrative perspective, improvements must be made to the individual items and indicators. It is expected that if security system indicators such as firewalls, intrusion detection systems, and data loss prevention systems that were not considered in this study are added, a more powerful diagnostic tool can be developed. If future studies supplement this study's questionnaire by expanding the list of items, they may be able to develop a more meaningful diagnostic tool and perform further analyses, thereby deriving practical methods for improving the technology protection capabilities of an organization.

Author Contributions: Data curation, Formal analysis & Writing-Original Draft Preparation, H.P.; Writing—Original Draft Preparation, Y.Y.; Conceptualization, Methodology, Funding acquisition & Writing—review & editing, H.L. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea (NRF-2018S1A5A8027174); This work was supported by the growth support project for industrial innovation talent of MOTIE.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Park, S.; Kim, Y.; Park, G.; Na, O.; Chang, H. Research on digital forensic readiness design in a cloud computing-based smart work environment. *Sustainability* **2018**, *10*, 1203. [CrossRef]
2. Ferry, J. Top Five Cases of Huawei IP Theft and Patent Infringement. Available online: https://www.prosperousamerica.org/top_five_cases_of_huawei_ip_theft_and_patent_infringement (accessed on 21 June 2021).
3. Ferry, J. Top Ten Cases of Chinese IP Theft. Available online: https://www.prosperousamerica.org/top_ten_cases_of_chinese_ip_theft (accessed on 21 June 2021).
4. Parker, H. Knowledge acquisition and leakage in inter-firm relationships involving new technology-based firms. *Manag. Decis.* **2012**, *50*, 1618–1633. [CrossRef]
5. Chang, H.-B. The design of information security management system for SMEs industry technique leakage prevention. *J. Korea Multimed. Soc.* **2010**, *13*, 111–121.
6. Kim, J.; Lee, C.; Chang, H. The Development of a Security Evaluation Model Focused on Information Leakage Protection for Sustainable Growth. *Sustainability* **2020**, *12*, 10639. [CrossRef]
7. Waterman, R.H.; Peters, T.J. *In Search of Excellence: Lessons from America's Best-Run Companies*; Harper & Row: New York, NY, USA, 1982.
8. Chen, J.-X.; Liu, W. Research on operational risk management framework for commercial banks in Internet world-based on McKinsey 7S model. In Proceedings of the 2010 International Conference on Internet Technology and Applications, Wuhan, China, 20–22 August 2010; pp. 1–6.
9. Gechkova, T.; Kaleeva, T. The mckinsey 7s model in the airport system protection. *Knowl. Int. J.* **2020**, *42*, 843–848.

10. Peteraf, M.A.; Bergen, M.E. Scanning dynamic competitive landscapes: A market-based and resource-based framework. *Strateg. Manag. J.* **2003**, *24*, 1027–1041. [CrossRef]
11. Miyazaki, K. *Building Competences in the Firm: Lessons from Japanese and European Optoelectronics*; Springer: Berlin/Heidelberg, Germany, 2016.
12. Eisenhardt, K.M. Making fast strategic decisions in high-velocity environments. *Acad. Manag. J.* **1989**, *32*, 543–576.
13. Korean National Police Agency. Available online: https://www.police.go.kr/index.do (accessed on 21 June 2021).
14. Stone, D.L.; Deadrick, D.L.; Lukaszewski, K.M.; Johnson, R. The influence of technology on the future of human resource management. *Hum. Resour. Manag. Rev.* **2015**, *25*, 216–231. [CrossRef]
15. Korean Intellectual Property Office. *Manual for Trade Secret Management*; Korean Intellectual Property Office: Daejeon, Korea, 2011.
16. Ministry of Trade Industry and Energy. *Industrial Technology Protection Guidelines*; Ministry of Trade Industry and Energy: Sejong, Korea, 2021.
17. Ministry of SMEs and Startups. *Technology Protection Guidelines for Small and Medium-Sized Enterprises*; Ministry of SMEs and Startups: Daejeon, Korea, 2018.
18. Swanson, M. *Security Self-Assessment Guide for Information Technology Systems*; Booz-Allen and Hamilton Inc.: Mclean, VA, USA, 2001.
19. Office of the Government Chief Information Officer. *Practice Guide for Security Risk Assessment & Audit [ISPG-SM01]*; Office of the Government Chief Information Officer: Wan Chai, Hong Kong, 2017.
20. Australian Cyber Security Centre. *Australian Government Information Security Manual*; Australian Cyber Security Centre: Kingston, Australia, 2021.
21. International Organization for Standardization. Available online: https://www.iso.org (accessed on 21 June 2021).
22. Hong, S.W.; Park, J.-P. Effective Management of Personal Information & Information Security Management System (ISMS-P) Authentication systems. *J. Korea Acad. Ind. Coop. Soc.* **2020**, *21*, 634–640.
23. Johansson, E.; Johnson, P. Assessment of enterprise information security-an architecture theory diagram definition. In Proceedings of the Conference on Systems Engineering Research, Hoboken, NJ, USA, 24 March 2005.
24. Bae, J.-M.; Kim, S.; Chang, H. A study on design direction of industry-centric security level evaluation model through analysis of security management system. *J. Soc. E Bus. Stud.* **2016**, *20*, 177–191. [CrossRef]
25. Eminağaoğlu, M.; Uçar, E.; Eren, Ş. The positive outcomes of information security awareness training in companies–A case study. *Inf. Secur. Tech. Rep.* **2009**, *14*, 223–229. [CrossRef]
26. Hunker, J.; Probst, C.W. Insiders and Insider Threats-An Overview of Definitions and Mitigation Techniques. *J. Wirel. Mob. Netw. Ubiquitous Comput. Dependable Appl.* **2011**, *2*, 4–27.
27. Wong, W.P.; Tan, H.C.; Tan, K.H.; Tseng, M.-L. Human factors in information leakage: Mitigation strategies for information sharing integrity. *Ind. Manag. Data Syst.* **2019**, *119*, 1242–1267. [CrossRef]
28. Lim, H.-c.L.; Kwon, Y.-h.; Park, S.-h.; Han, H.-j. Development of a Diagnosis Tool to Measure Enterprise Security Culture Using 7S Model and Competing Value Model. *Korean Manag. Consult. Rev.* **2017**, *17*, 183–192.
29. Von Solms, B. Information security—The fourth wave. *Comput. Secur.* **2006**, *25*, 165–168. [CrossRef]
30. Sullivant, J. *Building a Corporate Culture of Security: Strategies for Strengthening Organizational Resiliency*; Butterworth-Heinemann: Oxford, UK, 2016.
31. Bacal, R. Organizational conflict-the good, the bad, and the ugly. *J. Qual. Particip.* **2004**, *27*, 21–22.
32. Naipinit, T.; Kojchavivong, S.; Kowittayakorn, V.; Sakolnakorn, T.P.N. McKinsey 7S model for supply chain management of local SMEs construction business in upper northeast region of Thailand. *Asian Soc. Sci.* **2014**, *10*, 35–41. [CrossRef]
33. AlHogail, A.; Mirza, A. Information security culture: A definition and a literature review. In Proceedings of the 2014 World Congress on Computer Applications and Information Systems (WCCAIS), Hammamet, Tunisia, 17–19 January 2014; pp. 1–7.
34. Singh, A. A study of role of McKinsey's 7S framework in achieving organizational excellence. *Organ. Dev. J.* **2013**, *31*, 39–51.
35. Ravanfar, M.M. Analyzing Organizational Structure based on 7s model of McKinsey. *Glob. J. Manag. Bus. Res.* **2015**, *15*, 6–12. [CrossRef]
36. Anderson, E.E.; Choobineh, J. Enterprise information security strategies. *Comput. Secur.* **2008**, *27*, 22–29. [CrossRef]
37. Modenov, A.; Vlasov, M. Organizational structure and economic security of an enterprise. *Rev. Espac.* **2018**, *39*, 22.
38. Antoni, C.H.; Baeten, X.; Perkins, S.J.; Shaw, J.D.; Vartiainen, M. Reward management: Linking employee motivation and organizational performance. *J. Pers. Psychol.* **2017**, *16*, 57–60. [CrossRef]
39. Furnell, S.; Clarke, N. Organizational security culture: Embedding security awareness, education, and training. In Proceedings of the IFIP TC11 WG, Moscow, Russia, 18–20 May 2005; pp. 67–74.
40. Odetunde, O.J. Influence of transformational and transactional leaderships, and leaders' sex on organisational conflict management behaviour. *Gend. Behav.* **2013**, *11*, 5323–5335.
41. Centre for the Protection of National Infrastructure. *Managing Security Risks throughout COVID-19*; Centre for the Protection of National Infrastructure: London, UK, 2021.
42. Pradhan, M.K.; Oh, J.; Lee, H. Understanding travelers' behavior for sustainable smart tourism: A technology readiness perspective. *Sustainability* **2018**, *10*, 4259. [CrossRef]
43. Henseler, J.; Ringle, C.M.; Sinkovics, R.R. The use of partial least squares path modeling in international marketing. In *New Challenges to International Marketing*; Emerald Group Publishing Limited: Bingley, UK, 2009.

44. Binsawad, M.H. Corporate Social Responsibility in Higher Education: A PLS-SEM Neural Network Approach. *IEEE Access* **2020**, *8*, 29125–29131. [CrossRef]
45. Abdi, H. Factor rotations in factor analyses. In *Encyclopedia for Research Methods for the Social Sciences*; Sage: Thousand Oaks, CA, USA, 2003; pp. 792–795.
46. Chin, W.W.; Johnson, N.; Schwarz, A. A fast form approach to measuring technology acceptance and other constructs. *MIS Q.* **2008**, *32*, 687–703. [CrossRef]
47. Chong, A.Y.-L.; Liu, M.J.; Luo, J.; Keng-Boon, O. Predicting RFID adoption in healthcare supply chain from the perspectives of users. *Int. J. Prod. Econ.* **2015**, *159*, 66–75. [CrossRef]
48. Foo, P.-Y.; Lee, V.-H.; Tan, G.W.-H.; Ooi, K.-B. A gateway to realising sustainability performance via green supply chain management practices: A PLS–ANN approach. *Expert Syst. Appl.* **2018**, *107*, 1–14. [CrossRef]
49. Zabukovšek, S.S.; Kalinic, Z.; Bobek, S.; Tominc, P. SEM–ANN based research of factors' impact on extended use of ERP systems. *Cent. Eur. J. Oper. Res.* **2019**, *27*, 703–735. [CrossRef]
50. Beckett, J.C. *Evaluating the Need for IT Security in the Small Medium Enterprise Sectors*; Texas A&M University: College Station, TX, USA, 2017.
51. Karlsson, M.; Denk, T.; Åström, J. Perceptions of organizational culture and value conflicts in information security management. *Inf. Comput. Secur.* **2018**, *26*, 213–229. [CrossRef]
52. Herath, T.; Rao, H.R. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decis. Support Syst.* **2009**, *47*, 154–165. [CrossRef]
53. Solomon, J.; Solomon, A.; Park, C.Y. The evolving role of institutional investors in South Korean corporate governance: Some empirical evidence. *Corp. Gov. Int. Rev.* **2002**, *10*, 211–224. [CrossRef]