sustainability

Article

Smart City Development in Taiwan: From the Perspective of the Information Security Policy

Yung Chang Wu [1,2], **Rui Sun** [1] **and Yenchun Jim Wu** [3,4,*]

[1] College of Business Administration, National Huaqiao University, Quanzhou 362021, China; 103081@webmail.nou.edu.tw (Y.C.W.); sunrui@hqu.edu.cn (R.S.)
[2] Department of Business, National Open University, New Taipei City 24701, Taiwan
[3] Graduate institute of Global Business and Strategy, National Taiwan Normal University, Taipei 10645, Taiwan
[4] College of Management, National Taipei University of Education, Taipei 10671, Taiwan
* Correspondence: wuyenchun@gmail.com; Tel.: +886-02-7749996

Received: 1 March 2020; Accepted: 4 April 2020; Published: 6 April 2020

Abstract: A smart city is developed through the Internet of Things (IoT), cloud computing, big data, mobile Internet, and other new generation technologies regarding information and communication, and data resources in various fields are integrated and applied. The issue of information security in the network era is the strategic focus, as well as the focus of people's attention, during Taiwan's smart city construction. Information security policies are the information security guidelines for organizations, and are key to the organization's information security performance; moreover, such policies show the organization's support and commitment to the information security of smart cities. This paper discusses the model of information security policy in Taiwan's smart cities, uses Path Analysis to explore the characteristics of information security policy in smart cities, and examines the relationship between the formulation, implementation, maintenance, and effectiveness of information security policies. Furthermore, this study examines the impact on the effectiveness of organizational information security policies and information security performance from the following aspects: The length of information security policy publication time, policy review, policy advocacy, employee compliance, fair law enforcement, etc., which are all concrete manifestations of the formulation, implementation, and maintenance of information security policy models. Through a questionnaire survey, the correlation between various assumptions, as well as the relationship between organizational information security characteristics, information security policies, and the effectiveness of information security, are verified one by one during the implementation of information security policies. Finally, conclusions and implications are put forward.

Keywords: smart city; information security effectiveness; information security policy; path analysis

1. Introduction

1.1. Relationship between Smart City and Information and Communication Technology

A smart city is a new concept and new mode that uses new-generation information technologies, such as IoT, cloud computing, big data, mobile Internet, and spatial geographic information integration to promote intelligent urban planning, construction, management, and service. Its content is to build up a smart government, smart people's livelihood, and smart production. First of all, a smart government develops and utilizes government information resources and establishes a database of government information resources. Second, smart people's livelihood helps improve the level of urban management and expands public services and business applications. Finally, smart production creates new industrial values and forms sustainable industrial support. The construction of smart cities has risen quietly [1]. The introduction of the smart city concept to Taiwan has garnered considerable attention from the government and corporations and has been regarded as a critical opportunity to realize sustainable urban development. The fundaments of smart cities are primarily based on the development and application of Information and Communication Technology (ICT), which crosses various disciplines and fields [2]. It encompasses the comprehensive utilization of new-generation ICT, such as IoT data collection, cloud computing, big data applications, Artificial Intelligence (AI), and mobile network transmission. Therefore, a well-developed information security policy (ISP) is essential [1]. In smart cities, ICT is used to conduct real-time computing and processing of data related to residents and objects in the city and satisfy the needs of various applications [3]. Based on the comprehensive utilization of new-generation ICT, smart cities thoroughly adopt the core technologies and applications of IoT data collection, big data mining and analysis, and cloud computing services [4] to develop novel development models for future cities.

1.2. Relationship between Smart Cities and Information Security

A smart city is an inevitable trend in the development of city informatization. It is the internal demand for the sustainable development of the city. Its core is the deep integration of information technology and urban development, by providing various intelligent information services, improving the living environment quality of urban people, optimizing urban management, production, and lifestyle, and enhancing the happiness of urban residents [5].

In the construction of a smart city, we should make use of the most advanced information technology to fully perceive the elements and operating state of the city, establish information interaction and processes between people and things, as well as between things and things, and mine the connection rules between systems through massive information collection, storage, and analysis. How to ensure the safety of such data and information is a major issue that smart cities must be cautious about.

The construction of a smart city should also truthfully evaluate the city's advantages and disadvantages, as well as the opportunities and challenges it faces. Centering on key assets and fields, information security is indispensable and important content that can achieve the goals of economic growth and social progress under the support of technology [6].

1.3. Intelligent Application

Smart government affairs, smart transportation, smart education, smart medical care, smart home, smart park, etc. are all part of the construction of smart cities. The smart city applications are closely related to business and livelihood problems [7]. Therefore, comprehensive information security concepts are crucial. However, the development of digitized smart cities poses severe information security challenges; any type of information security problem can engender catastrophic consequences that greatly impact resident livelihood. To increase the breadth, depth, and development speed of information security, the Taiwanese government plans to combine big data analysis and AI technology to construct a multilevel intelligent information security system for government agencies, key infrastructure, and local governments' regional governance. The system purpose is to predict trends in information security attacks and increase response speed to information security incidents [8], both of which are dependent on the guidance of and compliance with complete ISP [9].

1.4. Information Security Policy

Information security policies provide rules for protecting an organization's information assets; thus, the managers of all relevant communities (including general staff, information technology, and information security) must take policies as the basis for all information security plans, designs, and deployments. Policies should be introduced for guidance regarding how to solve problems and how technology should be used. Information regarding the correct use of equipment or software that is not specified in the policy should be included in the documents regarding the standards, processes, and principles of user manuals and system documents [10].

Information security policies are designed and planned layer by layer from top to bottom. Senior administrators should formulate policies to standardize various issues, and then, extend the formulation of operating procedures, processes, and specifications. According to NIST SP800-14, three levels of information security policies are defined, where the upper level is Enterprise information security policies (EISP), the middle level is Issue-specific security policies (ISSP), and the lower level is Systems-specific security policies (SysSP) [11].

EISP is the general name of the overall enterprise security policy, organizational security policy, IT security policy, or information security policy that belong to the upper level. EISP is based on and directly supports the mission, vision, and direction of an organization, and sets the strategic direction, scope, and keynotes for all security factors. It is also intended to solve overall compliance problems to ensure that the planning requirements and responsibilities assigned to various organizational components are met. In addition, it regulates the use of specific penalties and disciplinary actions.

The middle-level ISSP policies are the security policies that guide employees to correctly use various technologies and processes when the organization implements them to support routine operations, such as the use of email regulations, Internet access regulations, the prevention of computer viruses, and other related security policies.

SysSP usually acts as a standard or process to be used when configuring or maintaining a system, and is divided into two categories: (1) Management operation specifications; and (2) technical operation specifications—which clearly define the steps and sequences for executing operations.

To maintain the legality and viability of an information security policy, the security policy must have a responsible unit or person in charge, a review schedule, a method of putting forward review recommendations, and a date for the release and revisions of the strategy.

Preventive information security measures must encompass management, technical, and physical [12]. Thus, a well-developed ISP is a vital element for smart city players to establish information security management systems [13]. These players propose implementation directions and technical support commitments for information security management based on their operating requirements, relevant government regulations, and customer contract requirements [14].

The construction of smart cities should be carried out in a progressive manner. When technology-centered planning is conducted, if the top-level security policy framework is not fully planned, and the wide influence of security, management, and social fields is not considered, the security standards for the information flow of various applications in smart cities will exist in name only. New data usage is continuously connected with smart cities. Only by formulating information security policies can the effectiveness of information security be improved, which will bring continuous and far-reaching benefits to citizens. Therefore, the relationship between organizational information security characteristics, information security policies, and information security effectiveness is the main objective of this paper.

2. Construction of Information Security Infrastructure for Smart Cities in Taiwan

When digital risks surface in large quantities by means of complex systems, the hazard they generate is not an increase in damage, but a runaway collapse, or an abrupt transition to a novel and suboptimal state [15]. ISPs are the highest guidelines for the information security of smart cities [16]; a well-developed ISP can ensure the city's sustainable development, enhance residents' quality of life, and produce insights using data.

2.1. Smart City Technology Architecture

From the perspective of literature and practice, a smart city requires a complex system, and its construction and development have a long way to go. From the technical level, a smart city is divided into four levels of elements and three support systems [17]. The four levels of elements are the IoT perception layer, network communication layer, service convergence layer, and intelligent application layer. The three major support systems are standard system, safety guarantee system, and construction management system.

On the basis of adhering to the overall situation of an urban development strategy and strengthening the top-level design, in the current period, efforts should be made to start from the basic level, deepen the understanding of the relevant theories and technologies of smart cities, and accelerate the process of urban wisdom, as based on scientific methods [18].

2.2. Current Situation of Information Security Planning for Taiwan's Smart Cities

A thorough ISP is the cornerstone of effective information security performance management in smart cities. Taiwan has developed the information security industry into a digital industry and mandated that competent authorities related to key infrastructures must establish their own respective platforms for information security, namely, Information Sharing and Analysis Centers (ISAC), Security Operation Centers (SOC), and Computer Emergency Response Teams (CERT) [19]. Subsequently, the smart city's information security intelligence system must be integrated and centralized to achieve its true value [20].

ISP frameworks of smart cities employ information security management, technology, and maintenance to achieve the long-term goal of constructing an information security system [21]. For example, the smart city construction of Taipei City is centered on information security and accompanied by smart applications, such as smart education, smart transportation, smart innovation, smart health care, smart payment, and smart public housing. To access the shared information security platforms and information, players in the construction of smart cities must adhere to the common standards and regulations stipulated in government-established ISPs. These policies guide the information security constructs in Taiwan's smart cities.

2.3. Information Support Technology for Smart Cities

A smart city is the product of the organic integration of a digital city with IoT, cloud computing, big data, and other technologies. Based on the basic framework of a digital city, various IoT sensors connect people and their related fixed or mobile items, and transfer the storage, calculation, and interactive services of massive data to the cloud computing platform for processing, in order to implement real-time automatic control of the city according to the processing results, and provide city managers and city residents with access anytime and anywhere. In this way, smart city services can be realized [22]. Therefore, from a technical point of view: Smart city = digital city + cloud computing + big data + IoT + mobile network + information security.

3. The ISP Model for Smart Cities

ISP contents must include the minimum requirements and principles, a definition of information security, maintenance and implementation measures, its information security hierarchy, and an investigation of its depth [23]. International Organization for Standardization/International Electro technical Commission (ISO/IEC) stipulates that ISPs must include a content description on the ISP and how an organization is to implement the ISP [24]. ISPs must be approved by the head of an organization, announced and communicated, and regularly reviewed and evaluated.

ISP characteristics are directly related to the information security requirements of smart city players. These characteristics influence the relationship between the players and the smart city's ISP model. Questions to consider whether different smart city ISP characteristics influence the smart city's ISP models, and whether different ISP characteristics can be used to understand, explain, and predict the planning of smart city's ISP models.

The literature on the security policy theory for information security management argues that smart cities can achieve information security by formulating and implementing information security management policies [1]. An ISP model [25] can be explored from several dimensions, namely, ISP announcement timing, the ISP review, ISP campaign, employee compliance, and fair enforcement. These constructs represent the formulation, implementation, and maintenance of an ISP model. A question to consider is whether these constructs increase the smart city's ISP effectiveness.

Smart cities use ISPs to ensure that their information assets are secured according to the CIA principles (i.e., confidentiality, integrity, and availability). This study adopted the contingency theory as a theoretical basis [26] to analyzed ISP models. A research framework was constructed to verify whether a smart city's ISP characteristics or model affected the increase in information security effectiveness and to understand the following: (1) The influence of a smart city's ISP characteristics on its ISP formulation, implementation, and maintenance; (2) the influence of ISP models on enhancing information security efficiency; and (3) the causal relationships between the aforementioned items.

3.1. Formulation, Implementation, and Maintenance of ISP

(1) Formulation: The key purpose of ISP is to define the core values of the smart city's ISP. Smart cities that employ different asset management methods have different information security core values; a smart city's ISP should conform to the core values of its information security strategies. In addition, smart cities should determine their information asset value to enhance the feasibility of its ISP [27].

The ISP implementation comprises the following stages: The establishment of a project team at the beginning of the project; formulation of detailed ISPs according to the information security theory and the smart city's needs for information asset protection; approval of consultation and authorization procedures by the board of directors and competent authorities of the smart city; security awareness and ISP education; and ISP promotion campaigns [28].

(2). ISP Implementation Content: ISPs must comprise the following: A definition of its overall objective and scope; a statement on the importance of security when sharing information; a description and explanation of the ISP; information security principles and standards; regulations that employees must comply with (including legal requirements and other regulations); requirements for information security awareness education and training; requirements for computer virus prevention; plans for sustainable operation; ISP violation consequences; description of the smart cities' responsibilities and division of labor for information security tasks; employees' general and specific information security responsibilities; and emergency notification procedures, handling procedures, and relevant regulations and instructions in the event of information security incidents [13].

ISPs are generally multilevel security concepts [29]. In addition, international information security standards adopt different regulations regarding ISP content, as depicted in Table 1.

(3) Evaluation and Maintenance: To ensure information security, smart cities usually adopt various control management and evaluation measures [31]. Among these measures, the ISP is prime and serves as the foundation for implementing information security management. The adequacy of implementation and maintenance has an immensely far-reaching impact on the information security of smart cities [32]. For example, the protection of assets is the ultimate objective of the entire information security management system, particularly of key assets that affect operations. Similarly, smart cities must understand the assets, and attributes of the assets, that they are protecting [33].

Table 1. Elements and Characteristics of International Standards Related to Information Security.

Elements and Characteristics	ISO/IEC 17799	BSI*	COBIT*	GASSP*	GMITS*
Information security scope and requirements	X	X	X	X	
Information security goals	X	X			
Definition of information security	X				
Management's commitment to information security	X	X		X	
ISP approval					
ISP goal					
Information security principles	X	X			X
Compliance with legal regulations and contracts	X				X
Use of information asset security awareness and training	X	X			
Virus prevention and detection	X				X
Sustainable operation plan	X				X
System development and acquisition					X
Risk management					X
Personnel management					X
Outsourced management					X
Security-incident handling					X
Information classification					
Access control					
Roles and responsibilities	X	X	X	X	X
Disciplinary regulations for ISP violations	X	X	X		X
Supervision and review					
Announcement and commitment					
Reference and appendix	X				

Data source: Hone and Eloff (2002) [30]; compiled by the present researchers. * British Standards Institution (*BSI*); control objectives for information and related technology (COBIT); generally accepted system security principles (*GASSP*); guidelines for the management of IT security (GMITS); information security policy (ISP).

3.2. Key Tasks for Implementing Information Security Policies

The information security policy of a smart city is a key to link laws with personal moral choices, and personal moral choice behavior is naturally affected by information security policy norms, because of the tasks assigned in a smart city. The following tasks should be implemented so that the information security policy of smart cities may affect citizens' moral choices.

First, the announcement of security policies, including physical documents, and website announcements, allows all citizens to freely read the relevant regulations. Second, the review of security policies and the documents published by smart cities must enable all citizens to read and provide opinions. Third, in terms of policy advocacy, staff must adopt education and training and different advocacy methods to enable the public to fully understand the relevant contents, and when necessary, they must carry out appropriate tests to verify the public's understanding of the information security policy of smart cities. Fourth, regarding staff compliance, when citizens understand the contents of the information security policy for smart cities, they must identify with the contents of the policy and comply with the required code of conduct documents. Finally, concerning fair law enforcement, when citizens violate the information security policy, the smart city law enforcement units should fairly implement the punishment stipulated by the law. Only when the requirements of the policy are fairly implemented can the information security policy be implemented.

3.3. Research Model and Framework

Based on the contingency theory, this study integrated four information security management activities—namely, information security policy, risk management, internal control, and information audit—and designed the basic model of information security policy, taking into account discussions of Safa et al. [34] and Moody et al. [35] on information security policy. When responding to the demands of the environment and smart city business, smart cities can start from any of the aforementioned management activities and adopt different information security contingency management strategies—such is the contingency process [13].

The basic composition of this model comprises ISP characteristics; the formulation, implementation, and maintenance of the ISP model; and the increase in information security effectiveness. Their relationships are as follows: A smart city's ISP characteristics depicts its information security needs, affects ISP models, and increases information security effectiveness, as shown in Figure 1.

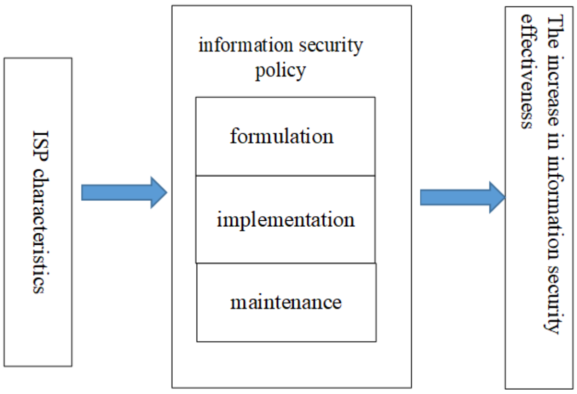
ISP characteristics
information security policy
formulation
implementation
maintenance
The increase in information security effectiveness

Figure 1. Basic ISP model.

Furthermore, their functional relationship is as follows: ISP model = f (smart city's ISP characteristics); and the increases in information security effectiveness = f (formulation, implementation, and maintenance of the ISP model). Subsequently, the research framework for ISP models for smart cities was established, as shown in Figure 2.

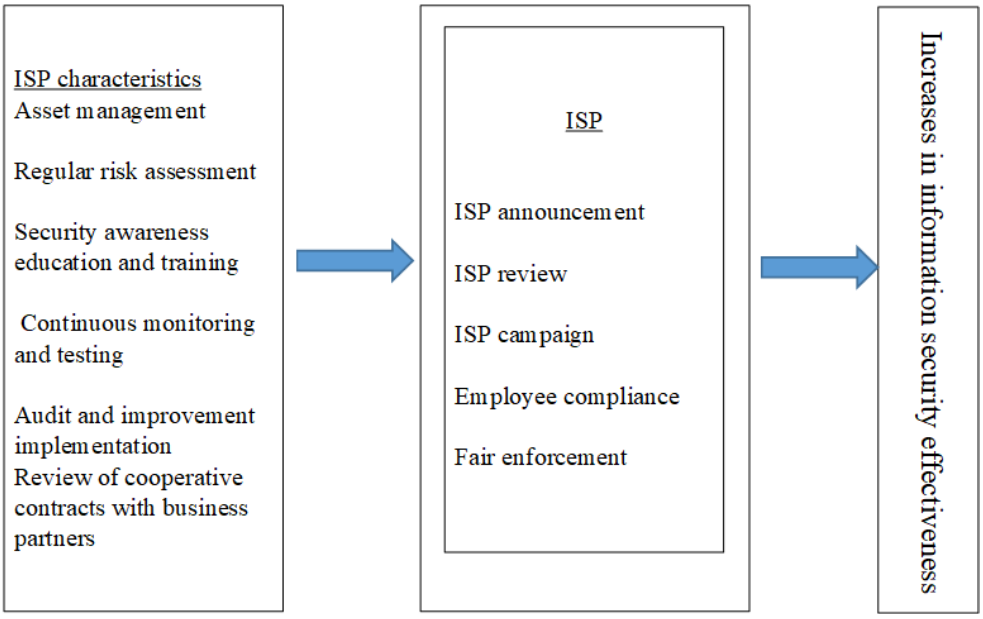
ISP characteristics
Asset management
Regular risk assessment
Security awareness education and training
Continuous monitoring and testing
Audit and improvement implementation
Review of cooperative contracts with business partners
ISP
ISP announcement
ISP review
ISP campaign
Employee compliance
Fair enforcement
Increases in information security effectiveness

Figure 2. The research framework for ISP models.

Figure 2 indicates that the researchers examined the influence of the smart city's information security needs on the formation of the smart city's ISP model and whether the formulation, implementation, and maintenance of ISP models increase the information protection effectiveness. In other words, this study examined whether the information security needs of smart cities increased information security effectiveness via the formulation, implementation, and maintenance of ISP models [36]. The information security needs of a smart city are reflected in its ISP characteristics, which comprise the following constructs: Asset management, regular risk assessment [37], security awareness education and training, audit and improvement implementation, continuous monitoring and testing, and the review of cooperative contracts with business partners. The formulation, implementation, and maintenance of ISP models comprise the following constructs: ISP announcement, ISP model review, ISP model campaign, employee compliance, and fair enforcement. Subsequently, this study classifies the increases in information security effectiveness as a construct itself. The research framework of the ISP model is shown in Figure 3. The definitions of each construct are as follows:

- Asset management: The ranking and classification management of information assets in smart cities.
- Regular risk assessment: The smart city's regular execution of risk assessment operations.
- Security awareness education and training: The smart city's direct and indirect execution of security awareness and educational training activities to achieve the business objective of information security.
- Continuous monitoring and testing: The continuous monitoring and testing to ensure that the system conforms to CIA principles.
- Audit and improvement implementation: The audit of the information department or information system, as well as ameliorating weaknesses.
- Review of cooperative contracts with business partners: The effectiveness of contracts with computer software and hardware, data, network equipment, and other vendors outsourced by smart cities.
- ISP announcement: The announcement of ISP models formulated by smart cities.
- ISP review: The smart city's expected degree of compliance between its needs and the formulated ISP model.
- ISP campaign: The campaign of a smart city's ISP model and the primary content it comprises.
- Employee compliance: Employees' compliance with an ISP model.
- Fair enforcement: Procedures and methods for the implementation of an ISP model.

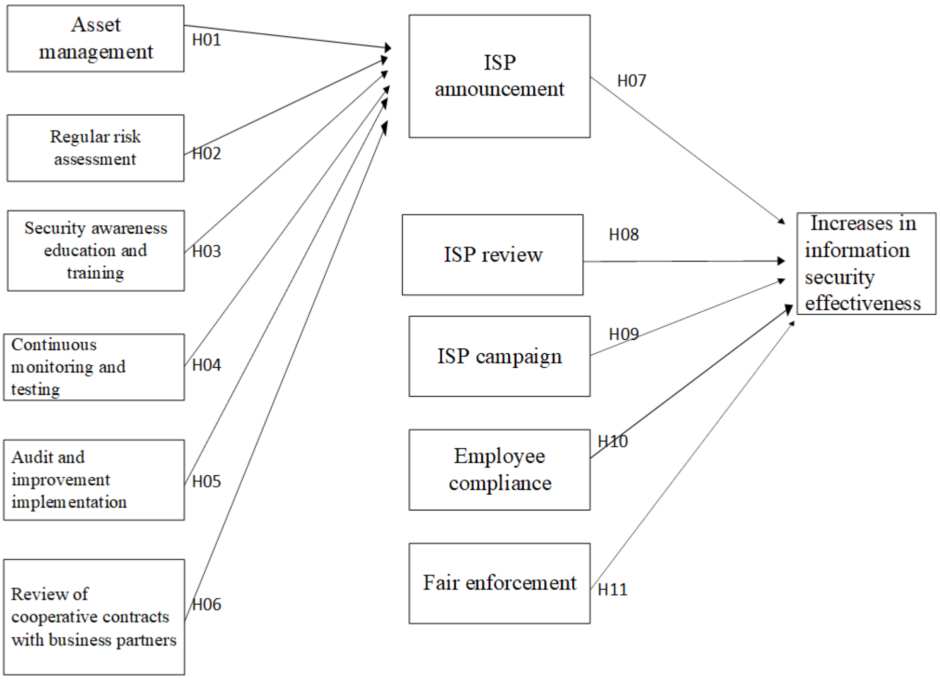
Asset management
Regular risk assessment
Security awareness education and training
Continuous monitoring and testing
Audit and improvement implementation
Review of cooperative contracts with business partners
H01
H02
H03
H04
H05
H06
ISP announcement
ISP review
ISP campaign
Employee compliance
Fair enforcement
H07
H08
H09
H10
H11
Increases in information security effectiveness

Figure 3. The research framework of the ISP model.

The influence of a smart city's information security by the formulation, implementation, and maintenance of an ISP model. This encompasses the reduction of threats or vulnerabilities, security incidents, security incident losses, and the shortened recovery time following security incidents, as well as increases in overall information security performance.

Practical observations and literature discussion have revealed that smart cities with different industries have different information security needs, and generally possess adopts different viewpoints and practices in the formulation of ISP models [38]. Specifically, smart cities with different ISP characteristics are influenced differently by ISP announcement timing and decision-making processes related to ISP formulation. Because of the different aims of smart city establishment, differences in the scope of regular risk assessments, security awareness and educational training, continuous monitoring and testing, and the review of cooperative contracts with business partners have different influences on the decision-making process for information security formulation [39]. Therefore, regarding the decision-making process of information security management, this study argued that ISP characteristics affected the timing of ISP announcements [40], and proposed the following hypotheses (H1–H6) for verification.

Hypothesis (H1). *Different types of information asset management have an impact on ISP models.*

Hypothesis (H2). *Smart cities that perform regular risk assessments formulate ISP models earlier.*

Hypothesis (H3). *Smart cities that implement security awareness education and training formulate ISP models earlier.*

Hypothesis (H4). *Smart cities that perform continuous monitoring and testing formulate ISP models earlier.*

Hypothesis (H5). *Smart cities that perform audits and improvements formulate ISP models earlier.*

Hypothesis (H6). *Regular reviews of cooperative contracts with business partners have an impact on ISP models.*

ISP models are a part of a smart cities' ISP, and serves as the highest guiding principle and infrastructure of information security. Smart cities usually establish ISP models to form a consensus on information security inside and outside of the city. This consensus marks the baseline level of information security set by smart cities and serves as their common goal for information security. The following are sufficient for affecting an organization's information security performance: The definition of the scope of information security, setting of information security goals and strategies, each level's information security responsibilities and regulations, supervision of compliance with information security mechanisms, and the announcement of consequences for noncompliance with information security guidelines [41,42]. Therefore, the present study argued that ISP announcement timing, as well as the ISP review, affects the increases in information security effectiveness, and proposed the following hypotheses (H7–H11) for verification.

Hypothesis (H7). *ISP model announcements affect increases in information security effectiveness.*

Hypothesis (H8). *ISP model reviews affect increases in information security effectiveness.*

The focus of an ISP model is in its implementation; that is, to implement the content outlined in the ISP model. ISP models comprise the following: The ISP goal, establishment and control of information security standard operating procedures, combination of information security and business operations, establishment of security awareness and enhancement of the range of application of coordination and integration, and implementation methods. These are crucial contents of an ISP model and are influential to information security [42,43]. The present study, thus, argued that the ISP model campaign affects increases in information security effectiveness and proposed the following hypothesis for verification.

Hypothesis (H9). *The ISP model campaign affects increases in information security effectiveness.*

Employee compliance with the ISP, also referred to as sub-policy, is the core part of the ISP model. Detailed specifications for this are presented in ISO/IEC 17799 [43], and encompass the following: ISP formulation, safe smart cities and its responsibilities, personnel safety, information asset classification, physical and environmental security, system planning and operational safety, data and media security, encryption control, communication and network security, access control, system development and maintenance, continuous business operations management, ISP execution, and information audit policy. These have immense and far-reaching impacts on information security [42,44]. Therefore, this study argued that implemented projects of ISP models affected the increase in information security effectiveness and proposed the following hypothesis for verification.

Hypothesis (H10). *Employee compliance with ISP models affects increases in information security effectiveness.*

According to the integrated theory of information security management, information security is enforced through the formulation, implementation, and maintenance of ISP models. The enforcement process must be fair [45]. Therefore, the establishment, evaluation, and maintenance of an ISP model is a key part of this theory, which assumes a planning and evaluation role in management procedures, and naturally makes contributions to information security [29,41]. The present study argued that the fair enforcement of ISP affects the increase in information security effectiveness and proposed the following hypothesis for verification.

Hypothesis (H11). *Fair enforcement affects increases in smart cities' information security effectiveness.*

3.4. Data Collection and Analysis

(1) Questionnaire Design: This study adopted the questionnaire survey method. In addition to referring to literature related to information security, practical situations were observed, and the questionnaire was developed accordingly. After the first draft of the questionnaire was completed, it was sent to relevant scholars and practitioners for trial filling; these scholars and practitioners then provided comments regarding revisions. The questionnaire was organized and divided into three sections:

Section 1: Survey of basic information regarding information security and ISP to collect data on the formulation of ISP models for smart cities and the departments and personnel responsible for information security.

Section 2: Survey of ISP models to collect data on ISP models function, content, implemented projects, procedures and methods for establishment and maintenance, and information security performance.

Section 3: Survey of background information to collect data related to ISP characteristics.

(2) Data Collection: The questionnaire was employed to examine the chief information officers and information department personnel of the 10 leading commercial enterprises in Taiwan. After excluding duplicate portions, 250 copies of the questionnaire were sent by e-mail in October 2019. Excluding six invalid copies, 147 valid questionnaires were collected for an effective response rate of 58.8%.

(3) Research Tools: SPSS Statistics was employed to conduct various statistical analyses.

Frequency distribution: Descriptive statistics were performed using sample data.

Reliability measurement: Cronbach's α was used to measure the internal consistency of all questions in the same dimension, and thus, test their consistency.

Regression analysis: The functional relationship model of this research framework tested whether ISP characteristics (independent variable) significantly affect the ISP model (dependent variable), as well as whether the ISP model (independent variable) significantly affects information security efficiency (dependent variable), with the aim of examining their causal relationship. ISP characteristics were also employed to predict the ISP model formulation timing, and ISP models were employed to predict information security performance.

Path analysis: Path analysis was employed to understand the relationship between ISP characteristics, ISP models, and information security effectiveness. A recursive model was employed to investigate ISP characteristics, whereas, the formulation, implementation, and maintenance of ISP models were used to explain the increase in information security effectiveness.

(4) Data Analysis:

Analysis of the sample's basic information: The number of employees in an information department was between 50–500 people and the number of employees in an information security department was between 5–30 people. The sampled core information systems in smart cities had between 1–30 years of tenure, among which systems younger than 5 years had undergone rewriting or platform upgrades in recent years. In terms of computer system architecture, most enterprises possessed mainframe or open architecture systems. In recent years, the financial industry also largely began the implementation of cloud computing, big data platforms, and intelligent robots. Regarding smart city hierarchy in information security departments, enterprises remained that operated within an information department without being independent.

Reliability analysis: In this study, the Cronbach's α coefficient was used to measure the internal consistency of dimensions. Table 2 presents these coefficients and shows that all Cronbach's α values were greater than 0.8, satisfying the reliability standards of general statistics. The error variance of the dimensions exhibited high explanatory power, as well as high consistency. Therefore, the dimensions possess a high degree of reliability.

Table 2. Reliability analysis.

Variable	Question Number	Cronbach's α Value
ISP review	5	0.8252
ISP campaign	7	0.8722
Employee compliance	13	0.9446
Fair enforcement	13	0.9139
Increase in information security effectiveness	6	0.9317

4. Hypothesis Testing and Model Verification

4.1. Hypothesis Testing

(1) Effect of Smart City Strategy Characteristics on ISP:

This study proposed six hypotheses regarding the impact of smart cities' ISP characteristics on the formulated ISP. Among them, the following two hypotheses were supported by test results: H1, different types of information asset management have an impact on ISP models; and H5, smart cities that perform audits and improvements formulate ISP models earlier. The remaining four hypotheses—H2, H3, H4, and H6—were not supported, as shown in Table 3.

(2) Influence of Smart Cities' ISP Models on the Increases in Information Security Effectiveness:

Of the five hypotheses regarding the influence of smart cities' ISP models on the increases in information security effectiveness that were proposed, four were supported, namely, H8, smart cities' ISP models reviews affect increases in information security effectiveness; H9, ISP model campaign affects increases in information security effectiveness; H10, employee compliance with ISP models affects increases in information security effectiveness; and H11, fair enforcement affects increases in information security effectiveness. The remaining hypothesis, H7, was not supported, as shown in Table 3.

Table 3. Test results of the hypotheses.

Hypotheses	Regression Coefficient β	Hypothesis Test Results
H1: Different types of information asset management have an impact on ISP models.	0.163*	Supported
H2: Smart cities that perform regular risk assessments formulate ISP models earlier.	0.146	Not supported
H3: Smart cities that implement security awareness education and training formulate ISP models earlier.	0.106	Not supported
H4: Smart cities that perform continuous monitoring and testing formulate ISP models earlier.	0.122	Not supported
H5: Smart cities that perform audits and improvements formulate ISP models earlier.	0.181*	Supported
H6: Regular reviews of cooperative contracts with business partners have an impact on ISP models.	0.105	Not supported
H7: Smart cities' ISP model announcements affect increases in information security effectiveness.	0.006	Not supported
H8: The review of smart cities' ISP models affects increases in information security effectiveness.	0.506***	Supported
H9: The campaign of an ISP model affects increases in information security effectiveness.	0.273***	Supported
H10: Employee compliance with ISP models affects increases in information security effectiveness.	0.443***	Supported
H11: Fair enforcement affects increases in smart cities' information security effectiveness.	0.482***	Supported

* $p < 0.05$, *** $p < 0.001$.

4.2. Path Analysis

The restricted model of path analysis was employed to analyze relationships between the constructs of smart cities' ISP characteristics, models, and enhancement in information security effectiveness. The results are shown in Figure 4 and Table 4 and are explained as follows:

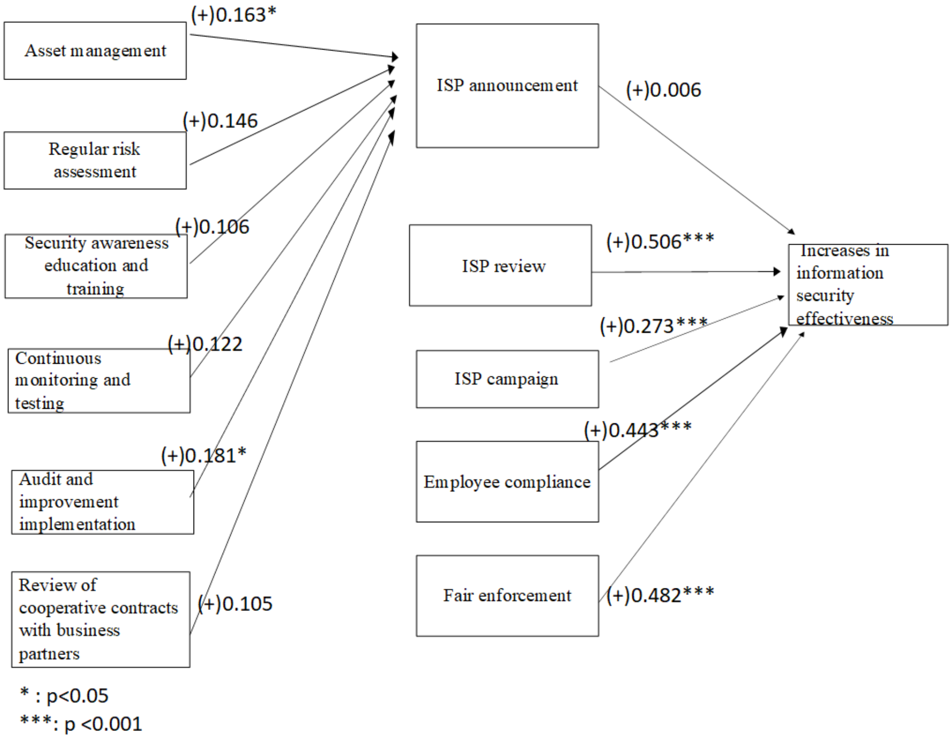

Figure 4. Path model of the ISP model.

Table 4. Regression results for predicting path relationships: Direct inference condition.

Independent Variable	Dependent Variable	R^2	F	b	t
Asset management	ISP announcement	0.026	4.189*	−0.163	−2.047*
Regular risk assessment	ISP announcement	—	—	—	—
Security awareness education and training	ISP announcement	—	—	—	—
Continuous monitoring and testing	ISP announcement	—	—	—	—
Audit and improvement execution	ISP announcement	0.033	5.204*	0.181	2.281*
Review of cooperative contracts with business partners	ISP announcement	—	—	—	—
ISP announcement	Increases in information security effectiveness	—	—	—	—
ISP review	Increases in information security effectiveness	0.256	53.454***	0.506	7.311***
ISP campaign	Increases in information security effectiveness	0.075	12.494***	−0.273	3.535***
Employee compliance	Increases in information security effectiveness	0.196	37.871***	0.443	6.154***
Fair enforcement	Increases in information security effectiveness	0.233	46.425***	0.482	6.814***

* $p < 0.05$, *** $p < 0.001$.

Asset Management: Analysis results indicated that asset management has a causal effect on ISP announcement. In other words, differences in asset management affect the ISP formulation time. The χ^2 test results revealed that the two constructs are significantly related ($p < 0.05$), thus, indicating that adequate asset management is closely related to the announcement of information security management guidelines.

Regular Risk Assessment: Analysis results indicated that regular risk assessment exhibited no causal effect on ISP announcements. In other words, no causal relationship exists between regular risk assessment and the announcement of smart cities' ISP. This may be due to the fact that regular risk assessment is a part of internal audit and internal control and is not positively correlated with the level of information security risk encountered by smart cities.

Security Awareness Education and Training: Analysis results indicated that security awareness education and training did not demonstrate a causal effect with ISP announcement. In other words, no causal relationship exists between security awareness education and training and the announcement of smart cities' security policies. Therefore, security awareness education and training do not affect smart cities' ISP announcements.

Continuous Monitoring and Testing: Analysis results indicated no causal effect between continuous monitoring and testing and ISP announcement.

Audit and Improvement Execution: Analysis results indicated that the execution of audits and improvements exhibited a causal effect on ISP announcement. In other words, a causal relationship exists between the execution of audits and improvements and ISP announcement. The χ^2 test results revealed that the two dimensions were significantly related ($p < 0.001$). This indicates that because many information security threats originate from within smart cities, the formulation of ISP models must be implemented accordingly to enhance smart cities' information security standards.

Review of Cooperative Contracts with Business Partners: Analysis results indicated that the review of cooperative contracts with business partners exhibited no causal effect on ISP announcement. In other words, no causal relationship exists between the review of cooperative contracts with business partners and ISP announcement. In the current information technology environment, information security issues persist in any information system architecture. Therefore, smart cities' ISP announcement timing is evidently unrelated to its review of cooperative contracts with business partners.

ISP Announcement: Analysis results indicated that ISP announcement exhibited no causal effect on the increases in smart cities' information security effectiveness. In other words, no causal relationship exists between a smart city's ISP announcement and increases in its information security effectiveness. Although appearing to be contrary to common sense judgment, the aforementioned result may be attributed to subsequent factors required for an ISP's functions, content, implementation, and maintenance to have a causal effect on information security effectiveness, such as whether the ISP is successfully implemented or if the ISP content satisfies the smart city's needs.

ISP Review: Analysis results indicated that the ISP model review exhibited a causal effect on the increases in smart cities' information security effectiveness. In other words, a causal relationship exists between the ISP model review and the increases in information security effectiveness. ISP models with greater competency to enforce within its information security scope, implement established goals and strategies, regulate the information security responsibilities of all levels, announce non-compliance consequences, and develop ISP implementation monitoring mechanisms yield greater increases in smart cities' information security effectiveness.

ISP Campaigns: Analysis results indicated that the ISP model campaign exhibit a causal effect on the increases in smart cities' information security effectiveness. In other words, a causal relationship exists between ISP model campaigns and smart cities' information security effectiveness. ISP model campaigns that emphasize on the following aspects yield greater increases in the smart city's information security effectiveness: ISP goals, security standards, operating procedures, establishment and regulation, the combination of information security and business operations, the establishment and enhancement of information security awareness, the coordination and integration of information security measures, the applicable scope of the ISP model, and implementation methods of information security measures.

Employee Compliance: Analysis results indicated that employee compliance exhibited a causal effect on the increases in smart cities' information security effectiveness. In other words, a causal relationship exists between employee compliance and the increases in smart cities' information security effectiveness, thus, indicating that employee compliance increases the smart city's information security effectiveness.

Fair Enforcement: Analysis results indicated that fair enforcement exhibited a causal effect on increases in smart cities' information security effectiveness. In other words, a causal relationship exists between fair enforcement and the increases in information security effectiveness. The fair enforcement of ISP that is more complete and exhaustive is more conducive to increasing information security effectiveness.

5. Conclusions and Suggestions

Information security is the cornerstone of the healthy development of smart cities. The continuous development of smart cities relies on comprehensive ISP guidelines that provide guidance in the development of safeguard mechanisms and systems. This study proposes an information security management strategy based on the contingency theory. By formulating, implementation, and maintaining ISP models, smart cities can adopt ISP models to shaping a PDCA cycle for information security management. Subsequently, smart cities can implement ISP models to achieve information security goals in accordance with the goals established in the ISP models.

5.1. Conclusions

Among the 11 research hypotheses proposed in this study, six were supported:

Specifically, asset management and the execution of audits and improvements affect the announcement of ISP models (H1, H5). In addition, ISP model review, ISP campaign, employee compliance, and fair enforcement collectively affect the increases in information security effectiveness (H8, H9, H10, H11).

The following four items were not significantly correlated with ISP announcements: Regular risk assessment (H2), security awareness education and training (H3), continuous monitoring and testing (H4), and the review of cooperative contracts with business partners (H6). An investigation into the causes for this lack of correlation indicated that these four items may be routine and normal operations that are not directly related to ISP announcements. Similarly, ISP announcement (H7) is a routine and standard information security procedure and is not directly related to a smart city's increases in information security effectiveness. This indicates that ISP models should emphasize substance over form.

In the process of building a smart city, the construction of information security is vitally important and is necessary for doing so for smart cities at the national level. It mainly includes the following six aspects [46].

- Establish and improve information security laws and regulations system, and promote the construction of information security and the rule of law.
- Establish and improve the organization and management mechanism of information security in intelligent cities, and strengthen the organization and guarantee of information security work.
- Establish an information security technology system for smart cities to realize independent and controllable information development.
- Build an information security infrastructure for smart cities, and provide support for information security capabilities.
- Establish and improve the information security standard system for smart cities, and strengthen the standardization of information security in smart cities.
- Establish an education system for training information security personnel, and speed up the construction of information security disciplines and the training of information security personnel.

The healthy development of smart cities depends on the guidance and standardization of information security policies. Information security in the construction of smart cities plays the following three roles [46].

First, to play a role in ensuring information security, from information security standards to information security strategies, from technical implementation to management measures, from the construction cycle to operation and maintenance, there must be elements to realize information security. Second, to play a gatekeeper role, the construction of a smart city information system should start from top-level planning, and a range of schemes should be formed through multi-level design and construction, acceptance, operation and maintenance, and other processes. These schemes usually need to be reviewed by experts and scholars before implementation. A detailed information security review can check on various plans for the construction of smart cities. Third, to play the role of authentication, generally speaking, the information system must pass the comprehensive evaluation and authentication of the information system before it can be put into operation. As the construction of smart cities mostly uses a series of high and new technologies, the difficulty and complexity of construction far exceed that of traditional information systems, and because each city has its own characteristics and is mostly built in innovation, there will be various unsafe factors. Therefore, only through certification can it be put into operation, which is a principle that must be strictly enforced.

This study proposed an ISP model based on security policy management strategies and strengthened compliance with laws and regulations. Verification results revealed the following: Separate causal relationships existed between ISP announcement and asset management or regular risk assessment; causal relationships collectively existed between ISP model review, ISP campaign, employee compliance, and fair enforcement with increases in information security effectiveness. In addition, larger information departments began the formulation of ISP models earlier. Smart cities with interests to increase its information security effectiveness should devote effort to strengthening essential constructs of the ISP model, such as IPS model review, ISP campaign, employee compliance, and fair enforcement [29].

5.2. Research Limitations

There are many risks in the construction of smart cities. The known challenges are the security risks faced by infrastructure, the security risks faced by IoT, the security risks faced by network communication, and the security risks faced by big data, cloud computing, and intelligent applications, which are comprehensive risks. However, the current research on information security is mostly limited to a single field and cannot meet the needs of interdisciplinary fields in smart city construction. This research comprehensively studied an information security policy, which can offer valuable contributions. We hope that future scholars can put forward more complete research reports that can be cited by practical circles.

Despite efforts to make this study rigorous, objective, and exhaustive, this research was limited by factors, such as human resources, material resources, and time. Some of these limitations were inevitable; for example, in the sample selection, this study directly examined enterprises that participated in the construction of Taiwan's smart cities and did not perform random sampling. This may have caused a decrease in external validity, thereby affecting the predictive capabilities of this study.

5.3. Implications

(1) Implications for Future Research:

Future studies should adopt random or stratified random sampling to increase external validity and further enhance their predictive capabilities. Future studies can increase the number of research constructs in accordance with the ISP theory to develop a more comprehensive research model of ISP models. For example, future studies can discuss the impact of actions taken by smart cities themselves or their component authorities on ISP models. By conducting empirical research on these topics, future studies can acquire more findings. Numerous theories related to information security management have been developed, such as risk management theory, institutional theory, strategic choice theory, and contingency theory [47]. Future studies can continue to develop research models for empirical research, which will greatly benefit the development of the information security management theory and practices.

(2) Implications for Practice:

To achieve information security goals, smart cities should establish ISP models and increase information security effectiveness by formulating, implementing evaluating, and maintaining of ISP models. The formulation of ISP models should focus on the substance of its policies, without excessive attention to the form. Enterprises that conduct larger-scaled regular risk assessments and have more information personnel are in greater need of ISP models. These models can serve as standards and benchmarks for personnel to abide by.

(3) Suggestions for Applications:

In every possible technology application in a smart city, the goal should be to create a place where decisions can be easily made, potential problems can be actively solved, and resources can be rationally allocated. When relying on a cohesive public safety system, we must consider the revolutionary impact of technology and the data we generate and consume in cities. How we build a smart city is the best summary of how we can most effectively connect people with the natural environment and the artificial environment [47].

The descriptions and verification results of this study provide an in-depth understanding of smart cities' information security policies and encompass the management, technical, and physical aspects. Therefore, the formulation of ISP models is the highest priority for corporations and smart cities. By establishing management regulations according to ISPs and successfully implementing ISPs, smart cities can lower information risks and improve their information protection capabilities.

Author Contributions: Conceptualization, Y.C.W., R.S. and Y.J.W.; methodology, Y.C.W.; software, Y.C.W.; validation, R.S. and Y.J.W.; formal analysis, Y.C.W.; investigation, Y.C.W..; resources, Y.C.W., R.S.; data curation, Y.C.W.; writing—original draft preparation; supervision, R.S.; funding acquisition, Y.J.W. All authors have read and agreed to the published version of the manuscript.

Funding: This study was in part supported by Ministry of Science and Technology, Taiwan (MOST 108-2511-H-003-034 -MY2).

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

References

1. Bifulco, F.; Tregua, M.; Amitrano, C.C.; D'Auria, A. ICT and sustainability in smart cities management. *Int. J. Public Sect. Manag.* **2016**, *29*, 132–147. [CrossRef]

2. Wu, Y.J.; Chen, J.C. A structured method for smart city project selection. *Int. J. Inf. Manag.* **2019**. [CrossRef]
3. Makoza, F. How and Why: A Decade of National ICT Policy Formulation in Malawi–A Historical Analysis. *Int. J. Inf. Commun. Technol. Hum. Dev.* **2019**, *11*, 38–65. [CrossRef]
4. Executive Yuan. *Sustainable Smart City-Smart Green Building and Community Promotion Program*; Executive Yuan: Taipei, Taiwan, 2016.
5. Chui, K.T.; Vasant, P.; Liu, R.W. Smart city is a safe city: Information and communication technology–enhanced urban space monitoring and surveillance systems: The promise and limitations. In *Smart Cities: Issues and Challenges*; Elsevier: Amsterdam, The Netherlands, 2019; pp. 111–124.
6. Jenab, K.; Moslehpour, S. Cyber security management: A review. *Bus. Manag. Dyn.* **2016**, *5*, 16–39.
7. El-kholei, A.O. Risks, hazards, and disasters: Can a smart city be resilient? In *Smart Cities: Issues and Challenges*; Elsevier: Amsterdam, The Netherlands, 2019; pp. 125–146.
8. Visvizi, A.; Lytras, M.D. Rescaling and refocusing smart cities research: From mega cities to smart villages. *J. Sci. Technol. Policy Manag.* **2018**, *9*, 134–145. [CrossRef]
9. Hongwei, J. *Analysis of Current Security Situation" Report*; Executive Yuan: Taipei, Taiwan, 2017.
10. National Institute of Standards and Technology. *An Introduction to computer Security: The NIST Handbook*; SP 800-12; NIST: Gaithersburg, MD, USA, 1995.
11. National Institute of Standards and Technology. *Generally Accepted Principles and Practices for Securing Information Technology Systems*; SP 800-14; NIST: Gaithersburg, MD, USA, 1996.
12. Bsi. ISO/IEC 27001: 2013 Your Implementation Guide. 2013. Available online: https://www.bsigroup.com/LocalFiles/en-GB/iso-iec-27001/resources/ISO-27001-implementation-guide.pdf (accessed on 20 February 2020).
13. Tajima, K.; Ishikawa, R.; Mori, T.; Suzuki, Y.; Takaya, K. A study on risk evaluation of countermeasure technique for preventing electromagnetic information leakage from ITE. In Proceedings of the 2017 International Symposium on Electromagnetic Compatibility-EMC EUROPE, Angers, France, 4–7 September 2017; pp. 1–4.
14. Jeong, D.Y.; Kim, G.; Lee, S. A Study on Risk Analysis and Countermeasures of Electronic Financial Fraud. *J. Korea Inst. Inf. Secur. Cryptol.* **2017**, *27*, 115–128.
15. Mclennan, M.; Group, Z.I. The Global Risks Report. 2020. Available online: https://www.weforum.org/reports/the-global-risks-report-2020 (accessed on 20 February 2020).
16. Berkel, A.R.R.; Singh, P.M.; Van, S.M.J. An information security architecture for smart cities. In *International Symposium on Business Modeling and Software Design*; Springer: Cham, Switzerland, 2018; pp. 167–184.
17. Van, Z.L. Privacy concerns in smart cities. *Gov. Inf. Q.* **2016**, *33*, 472–480.
18. Knapp, K.J.; Morris, R.F., Jr.; Marshall, T.E.; Byrd, T.A. Information security policy: An organizational-level process model. *Comput. Secur.* **2009**, *28*, 493–508. [CrossRef]
19. Lafuente, G. The big data security challenge. *Netw. Secur.* **2015**, *2015*, 12–14. [CrossRef]
20. Dameri, R.P. Smart city implementation. In *Progress in IS*; Springer: Genoa, Italy, 2017.
21. *Information Security Technology—Implementation Guide for Classified Protection of Information System*; GB/T25058; 2010; Available online: http://m.wdfxw.net/doc21620421.htm (accessed on 20 February 2020).
22. Gil-Garcia, J.R.; Pardo, T.A.; Nam, T. What makes a city smart? Identifying core components and proposing an integrative and comprehensive conceptualization. *Inf. Polity* **2015**, *20*, 61–87. [CrossRef]
23. Stimmel, C.L. *Building Smart Cities: Analytics, ICT, and Design Thinking*; CRC Press: Boca Raton, FL, USA, 2015.
24. Liang, J.; Huang, Y. Opportunities and challenges in technological development from digital cities to smart cities. *Geogr. Inf. World* **2013**, *20*, 81–86.
25. Shulan, C. Challenges of the information security sharing and analysis center-EU experience and china's challenges. *Technol. Law Anal.* **2018**, *30*, 47–59.
26. Wu, S.M.; Chen, T.; Wu, Y.J.; Lytras, M. Smart cities in Taiwan: A perspective on big data applications. *Sustainability* **2018**, *10*, 106. [CrossRef]
27. Tseng, B.; Chen, C.-Y.; Lin, I.-C. Information security talents. *Deep. Potential Inf. Secur. Talents* **2018**, *24*, 44–57.
28. Kolkowska, E.; Karlsson, F.; Hedstrom, K. Towards analysing the rationale of information security non-compliance: Devising a value-based compliance analysis method. *J. Strategic Inform. Syst.* **2017**, *26*, 39–57. [CrossRef]

29. Hong, K.S.; Chi, Y.P.; Chao, L.R.; Tang, J.H. An integrated system theory of information security management. *Inf. Manag. Comput. Secur.* **2003**, *11*, 243–248. [CrossRef]
30. Höne, K.; Eloff, J.H.P. Information security policy—What do international information security standards say? *Comput. Secur.* **2002**, *21*, 402–409. [CrossRef]
31. Goguen, J.A.; Meseguer, J. Security policies and security models. In Proceedings of the 1982 IEEE Symposium on Security and Privacy, Oakland, CA, USA, 26–28 April 1982; pp. 1–11.
32. Alqahtani, F.H. Developing an information security policy: A case study approach. *Procedia Comput. Sci.* **2017**, *124*, 691–697. [CrossRef]
33. Albino, V.; Berardi, U.; Dangelico, R.M. Smart cities: Definitions, dimensions, performance, and initiatives. *J. Urban Technol.* **2015**, *22*, 3–21. [CrossRef]
34. Safa, N.S.; Von Solms, R.; Furnell, S. Information security policy compliance model in organizations. *Comput. Secur.* **2016**, *56*, 70–82. [CrossRef]
35. Moody, G.D.; Siponen, M.; Pahnila, S. Toward a unified model of information security policy compliance. *MIS Q. Manag. Inf. Syst.* **2018**, *42*, 285-A22. [CrossRef]
36. Gupta, V.K. The parasitic hymenoptera and biological control of the African ichneumonidae. *Int. J. Trop. Insect Sci.* **1991**, *12*, 9–18. [CrossRef]
37. Wu, T.; Wu, Y.; Tsai, H.; Li, Y. Top management teams' characteristics and strategic decision-making: A mediation of risk perceptions and mental models. *Sustainability* **2017**, *9*, 2265. [CrossRef]
38. Cram, W.A.; Proudfoot, J.G.; D'Arcy, J. Organizational information security policies: A review and research framework. *Eur. J. Inf. Syst.* **2017**, *26*, 605–641. [CrossRef]
39. Wood, C.C.; Lineman, D. *Information Security Policies Made Easy Version 11*; Information Shield, Inc.: Houston, TX, USA, 2009.
40. Bulgurcu, B.; Cavusoglu, H.; Benbasat, I. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Q. Manag. Inf. Syst.* **2010**, *34*, 523–548. [CrossRef]
41. Gillibrand, W.; Flynn, M. Forced externalization of control in people with diabetes: A qualitative exploratory study. *J. Adv. Nurs.* **2001**, *34*, 501–510. [CrossRef] [PubMed]
42. Singh, A.N.; Gupta, M.; Ojha, A. Identifying factors of "organizational information security management". *J. Enterp. Inf. Manag.* **2014**, *27*, 644–667. [CrossRef]
43. Disterer, G. ISO/IEC 27000, 27001 and 27002 for information security management. *J. Inf. Secur.* **2013**, *4*, 92–100. [CrossRef]
44. Calder, A. *Nine Steps to Success: An ISO27001: 2013 Implementation Overview*; IT Governance Ltd.: Ely, UK, 2016.
45. Schwaig, K.S.; Kane, G.C.; Storey, V.C. Compliance to the fair information practices: How are the fortune 500 handling online privacy disclosures? *Inf. Manag.* **2006**, *43*, 805–820. [CrossRef]
46. Fan, Y. *Smart City and Information Security*, 3rd ed.; Publishing House of Electronics Industry: Beijing, China, 2017; pp. 17–79. ISBN 978-7-121-29815-8.
47. GFCIA. GFCA Whitepaper: Smart Cities Are All About People. 2018. Available online: https://www.prnewswire.com/news-releases/gfca-whitepaper-smart-cities-are-all-about-people-300649611.html (accessed on 20 February 2020).