JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Implementation of Advance Cyber Security Surveillance Framework with E Governance & Smart city

Mr. Jigul Nimavat [1], Dr.Vijaykumar B. Gadhavi[2]
[1]PhD Scholar – Computer Engineering Department Swaminarayan University, India,
Email id: jigulnimavat1987@gmail.com
[2]Associate Professor & Dean – Faculty of Engineering (I/C), Computer Engineering Department Swaminarayan University, India, vijaybgadhavi@gmail.com

ABSTRACT

Cybersecurity has proven to be a prominent topic in business and government developments. Although most Smart City organizations have cybersecurity strategies in place, they still face challenges in implementing them. The implementation and adoption of appropriate cybersecurity are challenging and knowledge-intensive and require the participation and support of policymakers and IT units. However, although awareness of critical success factors (CSF) for cybersecurity implementation is very beneficial in avoiding failure in Smart City projects, this area has rarely been researched, especially with a focus on Smart City development. Therefore, the contribution of this paper to research and practice is the identification of critical factors that influence the successful implementation of cybersecurity in smart cities. This study was carried out through an interview study with officials and staff in the Jakarta Smart City environment. As a result, we have 15 keys critical factor that has a practical implementation and could include in the model of cybersecurity in smart cities.

Keywords: *Critical Success Factors, Cybersecurity, Smart City, Security of Smart City*

1. INTRODUCTION

To implement smart cities relies heavily on computing technology, including cloud computing, where all information is available. Apart from being a source of information, cloud computing is also a means of storing data, and the failure to connect users, at the same time, will carry a very large security risk [1]. Security issues are non-technological and technological and occur in many forms. This condition will get worse because there are provider companies that do not prioritize cybersecurity. Consumers prefer low prices by ignoring the security threats that can be caused, therefore, provider companies do not prioritize cybersecurity [2].

In Indonesia, the National Cyber and Crypto Agency (BSSN) recorded that a total of 159 cases of cyberattack during the period January 1 to April 12, 2020, recorded 159 cases of website tampering on government websites [3].

The research data was collected from directors and decision makers in Jakarta smart city, to help generate realistic problems and obstacles around current developments, success factors and practices of cybersecurity initiatives that have been carried out by the Jakarta smart city. Furthermore, it provides a comprehensive picture of the real situation for cybersecurity implementation in Jakarta smart city. Jakarta Smart City was chosen to be the place for this research because Jakarta Smart City has been harmonized by the Jakarta Regional Government with the Sustainable Development Goals (SDGs) program [4]. Also, in the 2019 IMD World Competitiveness, the Jakarta Smart City was ranked 81, thus Jakarta Smart City has been recognized globally [5]. Another achievement achieved by Jakarta Smart City is becoming one of the ASEAN Smart City Urban Planning models at the Smart Cities Governance Workshop (SCGW) in Singapore on 22-25 May 2018 and receiving awards for implementing smart city and e- government in the 4th event World Cities and Cities Organization of Smart Sustainable Cities Award which was held on July 3-30 2017 in Ulyanovsk, Russia [6].

Be expected that Smart Cities will experience significant changes from the security aspect by implementing cybersecurity following the

characteristics of attacks in each smart city. It requires a cybersecurity model under the characteristics of attacks and bureaucratic flows in the government that houses the Smart City. The factors that are critical to developing a cybersecurity model should be identified. This paper has made an effort to identify the critical factors for the successful implementation of cybersecurity to develop a cybersecurity model in smart cities.

2. METHODOLOGY

A deductive approach has been used in this study to explore CSFs for cybersecurity implementation from the perspective of managers and decision-makers in smart city Jakarta. [7] have recommended a top-down approach to identify CSF because it can obtain specific confirmation of a particular hypothesis through literature and empirical findings. This research methodology has four stages that aim to identify CSFs for cybersecurity implementation in Jakarta smart city, which include; a) investigating existing models and factors of successful cybersecurity implementation, b) preparation process, c) process execution, and d) data analysis process. The detailed information about our methodology can see in Figure 1.

As shown in Figure 1, the first primary stage is to investigate existing models to determine common critical factors for cybersecurity implementation. The preparation process, including designing and compiling interview questions, developing trials and, modifying and analyzing the pilot interview questionnaire based on comments from respondents. This study uses the concept of template analysis by creating a list of codes ('templates') representing the themes identified in the textual data [8]. The initial template was created and guided by a series of questions for interviewing and setting high-level codes. The content of the interview questions covered cybersecurity issues faced by actors and policymakers in the Jakarta Smart City and the efforts made to overcome them. In the interview process, many new issues emerged and became new themes. Therefore, the initial template needs to be adjusted. Revisions the template makes the template could include all interview data. The third main stage is the implementation process, where this stage includes the selection of respondents from Jakarta smart city and interviews with respondents. The final stage is the analytical process, where we collect and analyze data to investigate CSFs related to the successful implementation of cybersecurity.

This study aims to find various critical success factors that influence the management and implementation of cybersecurity in Indonesia. Interviews were conducted with seven people from backgrounds consisting of the director of Jakarta smart city, the head of operations, the head of the code and cyber section, and four Jakarta smart city operational staff. The semi-structured informal interview style has been used as a medium to collect data for this study because this approach is flexible as it allows the researcher to ask new questions during and during the interview [9].

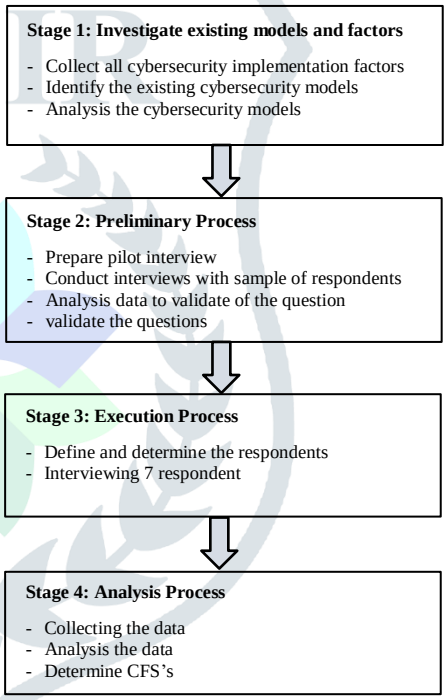

Figure 1. The Stages to Determine CSFs for Cybersecurity Implementation

3. DEFINITION OF CONCEPT

3.1 Implementation of Smart City

Smart City is defined as a city with a smart community that is independent and integrated through modern telecommunications infrastructure [10]. Over time, Information technology transforms traditional urban everyday life into smart and sustainable ways to make the quality of life, economy, and environment, more efficient and effective.

[11] describe a smart city as a city that integrates and monitors the state of all

infrastructure including bridges, tunnels, water, trains, subways, roads, airports, ports, communications, electricity, and all government buildings to optimize power resources and maximize security services for the citizens of the city.

With the development of computing technology and the smart city development activities in developed countries, many cities in developing countries have gradually initiated smart city initiatives by setting standards for their respective countries.

In Indonesia, several cities like Jakarta have adopted the smart city concept by optimizing existing resources and technology support. Jakarta Smart City has six pillars, namely Governance, Economy, People, Environment, Mobility, and Living [12]. Focusing on the six dimensions of the smart city is realized through service application programs. Until 2019, there are 25 Jakarta Smart City service application programs [13] [14], as in Table 1 below.

Table 1. Jakarta Smart City Application Services

Dimension	Applications
Smart Governance	1. Qlue 2. CROP 3. Public Information Disclosure Portal 4. Ragunan Zoo 5. Complaints Channel 6. CRM 7. API (Application Programing Interface) 8. Floods Monitoring 9. E-Musrenbang/ Plan JKT 10. E-Musrenbang/ Plan JKT 11. i-Jakarta 12. Nodeflux
Smart Mobility	1. Transjakarta "Smart Mobility for Smart city 2. Trafi 3. Waze 4. GoWes
Smart People	1. Indorelawan 2. JSC Hive Coworking Space 3. BERiDE
Smart Economy	1. Zomato 2. Gofood 3. Tokopedia 4. Jakmik
Smart Living	1. Foods Info Jakarta 2. Jakarta Safe
Smart Environtment	1. PJU LED Smart System

To gain recognition globally Jakarta smart city program must be in line with the SDGs program, although several sustainable SDG programs are still in the development stage [4].

Table 2 summarizes the programs in Jakarta smart city that aligned with the SDGs.

Table 2. Jakarta Smart City Program Aligns With SDGs

SDGs component	Jakarta Smart City Program
No Poverty	Home Loan Down Payment 0%
	Integrated Flats
Zero Hunger	Cheap Basic Food Cards
	Street Vendors Online
	Jakarta Food Info
Good Health and Well-Being	Jakarta Health Card
Quality Education	Jakarta Smart Card
	E-Jakarta
	Collaborative Space
Gender Equality	Provide Nursing Space in Public Areas
Clean Water and Sanitation	-
Affordable and Clean Energy	Subsidized Vehicle Gas and Fuel
Decent Work and Ecmonomic Growth	E-Budgeting
Industry, Innovation and Infrastructure	Jakarta One
	Transjakarta Application
	Public Space Lighting
	Electronic Parking
	CRM
	Open Data Program
Reduced Inequalities	-
Sustainable Cities and Communication	QlueMyCity
	PTSP in All Public Spaces
	PORTAL Jakarta
Responsible Consumption	3R Waste Management
Climate Action	Pollution Standard Index (Air Visual)
	Flood Monitoring
Life Below Water	-
Life on Land	-
Peace, Justice and Strong Institutions	-
Partnership for Goals	Establish Cooperation with Unicorns (Tokopedia and Gojek)

3.2 Smart City and Cybersecurity

Smart cities rely heavily on digital technology, including cloud computing, which provides much information. In addition to providing information, cloud computing is used to

store data and connect multiple users so that security risks cannot avoid [1]. Security problems can arise in several forms, and many cause, non-technological and technological causes. [2] states that in providing the smart city infrastructure such as IoT devices, provider companies do not prioritize cybersecurity because consumers prioritize low prices by ignoring security threats that can cause by devices that are not equipped with cybersecurity. Nearly 40% of fake transactions originating from mobile devices. Public services, finance, and information are the sectors most affected by these violations [15]. [16] found that some network sensys (econolites) devices used to control traffic lights in the US and Canada lack encryption, authentication, or security. Option errors when configuring signals and traffic and traffic light timing can occur because attackers can alter the signal with false data so that intersections in the US and Canada will be affected. Therefore, from a cybersecurity point of view, smart cities are seen as cities that supervise and consolidate all infrastructure with maximum security for the convenience of citizens [11].

As a developing country, Indonesia is a country with a weak level of cybersecurity. Indonesia experienced cyberattacks in second place after China, [17] noted that there had been 36.6 million cyber attacks in the past three years. One of them hackers tried to infiltrate the bank's customer card security system occurred in May 2014. It is a record of the weakness of cybersecurity in Indonesia [18].

Cyber attacks also experience by government institutions. Attackers can control government websites and use them for irresponsible purposes like changing the appearance of the web [17]. The Secretariat of One Data Indonesia recorded that the incident response statistics for the .go.id domain in 2020 saw an increase in web defacement attacks from 42 percent to 95 percent. Table 3 below provides incident response data for the .go.id domain in the year 2020.

Tabel 3. 2020 Domain .go.id Incident Response

Incident	Quarter			
	1st	2nd	3rd	4th
Web Defacement	42,0 %	66,8 %	75,0 %	95,0 %
Malware	35,0 %	14,5 %	2,0 %	00,0 %
Phising	17,0 %	8,9 %	1,0 %	1,0 %
Spam	5,0 %	9,4 %	17,0 %	1,0 %
DdOS	1,0 %	0,0 %	0,0 %	0,0 %
Brute Force	1,0 %	0,0 %	0,0 %	0,0 %
IPR	1,0 %	0,0 %	0,0 %	0,0 %
Bug	0,0 %	0,0 %	4,0 %	3,0 %
Data Leaked	0,0 %	0,0 %	1,0 %	0,0 %

The expansion of smart cities with modern technology has an increasing impact on cyberattacks, which is why smart cities need to plan and provide cybersecurity systems for future Smart City implementations. An important aspect that needs to be considered in the planning and development of Smart City security is to identify the critical success factors for cybersecurity in smart cities.

3.3 Defining Cybersecurity

Cybersecurity is an important issue for countries and organizations around the world as the use of information technology increases. The increased use of information technology and cybersecurity threats has a direct correlation. Cybersecurity threats are spreading in public and private sector organizations so that resources dedicated to advancing cybersecurity are experiencing a universal increase [19]. In business and governance globally, cybersecurity is a big challenge, because it is the center protection of all information technology assets from attack, damage, or unauthorized use [20]. Currently, some common problems can resolve with defense architecture and equipment, but they are not sufficient to overcome all possible threats. [21] notes that architecture and equipment are not the only parts of cybersecurity, people and processes are also components of cybersecurity.

Some research communities debate the exact definition of cybersecurity. [22] state cybersecurity is an attempt to defend digital systems from abuse and interference. In [23], cybersecurity is defined as cyber assets to maintain confidentiality, protect, and ensure the availability and integrity of information. [24] define cybersecurity as the protection of cyberspace itself, which supports cyberspace, and cyber users who are vulnerable to attacks originating from cyberspace.

In the field of cybersecurity, several discourses are mutually sustainable. Regarding legacy issues, the placement of the discussion in the “cyber” and “security” domains can be assisted in its placement by the deconstructed term cybersecurity [25].

In a general sense, the term "security" is difficult to translate because there is no really a widely accepted concept [24] [25]. [27] state that

the definition of security must include and try to understand who is securing, regarding the problems that occur (threats), to whom the problem is intended (object of reference), in what conditions and results (structure).

Of course, there are more definite forms of security (for example, information system properties, physical property, human property, or mathematical definitions for various types of security), based on what is a valued and individual point of view, that is what the term means. Although it was still debate, being free from danger or threat is the main principle of the definition of "security" [28].

The definition of cybersecurity from the perspective of cybersecurity materials as stated by the following researchers. [29] defines security as a defense method used to detect and thwart unauthorized access. Cybersecurity is the protection of information in computer networks from unauthorized users, damage, and harmful interference [30]. [31] notes that cybersecurity attempts to reduce the risk of malicious attacks on computer networks and software. It includes tools to detect attacks, block malicious access, remove viruses, enforce authentication, encrypt data. Cybersecurity is a collection of efforts and tools to protect the cyber environment and organizations and user assets from damage and unauthorized use. These efforts and tools are in the form of security concepts, guidelines, policies, security protection, risk management approaches, actions, training, best practices, assurance, and technology [32]. [33] defines cybersecurity as the art of guaranteeing and protecting critical information, assets, and infrastructure to ensure the existence and continuity of a nation's information society.

From some of the definitions in the literature above, [34] notes that cybersecurity is still a challenge that requires cross-disciplinary reasoning so that, any definition produced must be of concern to cybersecurity stakeholders so that it can use fundamentally.

3.4 Importance of Cybersecurity

The physical infrastructure of smart cities is interrelated because most of them are integrated into the network through information technology tools [35]. Data and information connected by devices have significantly impacted people's quality of life as never before [36]. At the same time, large amounts of connected data pose a privacy and security risk. The data available on the network can improve the quality of life and can also be stolen by hackers and used for illegal purposes.

Internet of Things (IoT) is widely adopted in everyday life, it can see from the increasing number of IP (Internet Protocol) addresses displayed by physical objects for internet connectivity as a means of communicating [37]. IoT contributes to creating a cyber-physical society that has a very high dependence on cyberspace, in every day is connected via a network using electronic devices and is at risk of becoming victims of cybercrime. Many cyber-physical communities perceive the internet as a safe environment and always use it through their cellphones or computers without realizing it a large number of cybercrimes and violations such as attacks and hacks occur to them [38]. The severe impact occurs in cyber-physical systems when intruders gain access to surveillance controls and take over control measures [35]. The risk is very high as a result of this action, intruders can take over control of all crucial assets such as flight controls, medical devices, auto propulsion cars, traffic systems, and power stations throughout the city and could pose a threat to life.

The dependence of the cyber-physical community on ICT is very large and tends to increase with technological developments and the passage of time so that the need for cybersecurity becomes increasingly crucial for individuals, public, and non-public organizations. Security issues are not limited to executive power but are also relevant to energy infrastructure providers, waterways, road management, political parties, ministries, administrative organizations, NGOs, all of which are targets of information breaches and theft [39].

Concerns for prevention and better investment in cybersecurity are not yet a priority, cybersecurity often focuses on how to deal with incidents after they occur [40]. Given the importance of cybersecurity issues, cybersecurity stakeholders must raise awareness and take drastic steps to ensure cybersecurity and security.

3.5 Type of Cybersecurity Threat

In order to understand how cyberattacks occur, a comprehensive analysis of the vulnerabilities and types of cybersecurity threats needs to identify. Several security threats can classify as physical threats, interception, misuse, and loss of information [41]. Introducing data tampering to gain unauthorized access to interfaces, leaking information by side channels, overpowering

central locking systems with error shots are all frequent physical threats.

As mentioned by [41] several threats facing Smart Cities can be classified as physical threats, interception, misuse, and loss of information. Reconnaissance, the man in the middle, and replay attacks on network-sent data internally between ECUs and between cloud users constitute interception threats. Traditional ICT attacks such as denial of service, unauthorized access, and malicious code execution.

Security threats classification by Uma and [42] is based on the purpose, scope, and severity of involvement. These classifications include denial of service attacks, access attacks, reconnaissance, active attacks, and passive attacks. [43] noted that security threats originate from aspects of authentication, hacking, viruses, availability, and message interception. Table 4 shows the types of attacks and related factors.

Table 4. Cybersecurity Threats and Related Factors

Attack Type	Factor Related		
	People	Technology	Process
Reconnaissance Attack		✓	
Access Attack	✓	✓	✓
Denial of service Attack		✓	✓
Active Attacks		✓	
Passive Attacks	✓	✓	
Malicious Large Scale		✓	✓
Non-Malicious Small Scale	✓		✓
Message Interception	✓	✓	✓
Authentication	✓	✓	✓
Hacking	✓	✓	
Viruses		✓	
Availability		✓	✓

Reconnaissance Attack: this is similar to theft accompanied by the destruction of lonely houses in residential areas. Reconnaissance attacks can consist of Scanning the Port, Packet Sniffers, Sweeping the Ping, and Queries about Internet Information.

Access Attacks: Access attacks consist of Secret Code Attacks, Port Redirection, Trust Port Utilization, Social Engineering, Phishing, and Man-in-the-middle Attacks. Illegal intruders are trying to gain access to devices that the intruder has no right to access. The intruder created tools to exploit hacked application vulnerabilities to obtain invalid entries into secret databases and other sensitive information.

Denial of service attack: The attacker deliberately destroys or disables network systems to stop service to users. Make the system unusable and even destroy the system by slowing down the system, destroying or deleting information.

Active Attacks: Attackers are on one of the communicating parties, so they can try to stop data from being sent by parties on the network. Attacks allow the attacker to send data to all parties or block data transmission in uni or multi-way manner.

Passive Attacks: Unauthorized users steal information by monitoring communications between two parties using a wiretapping system.

Malicious Large Scale: This attack caused the collapse of systems globally with the loss of large amounts of data and corporate credibility involving thousands of systems. Large-scale attacks can carry out by individuals or groups for personal gain or to create disturbance and chaos.

Non-Malicious Small Scale: This attack causes accidental damage due to an operational error by an untrained individual. However, the Non-Malicious Small Scale can cause data loss or system damage. Usually, only a small part of the system is compromised, and data can recovery.

Message Interception: An example of this attack is tapping to get data on the network and illegally copying a program or data file. This attack occurs because an unauthorized outside party has gained access to a network. The outsiders can be computing systems, programs, or people.

Authentication: Attackers use their own credentials to steal information on the network that not intend for them. This attack carries out by identifying the entity utilizing a username and password.

Hacking: Hacking is unauthorized access or control of computer network security systems to exploit computer systems or private networks.

Viruses: Software programs to perform malicious acts that are load onto the computer and the user is unaware.

Availability: Term used by storage service providers (SSPs) and computer storage manufacturers to describe products and services that ensure that data continues to be available at the level of performance required in situations ranging from normal to catastrophic.

Most cybersecurity policies will have a focus or purpose that draws on aspects of the

Confidentiality, Integrity, and Availability (CIA) triad. The CIA triad is a standard model in information security designed to regulate and evaluate how an organization or company is when data is stored, transmitted, or processed. Every aspect of the CIA triad will be an essential component of cybersecurity. Any attack in cyberspace will generally try to violate at least one aspect or attribute of the CIA triad. Several works of literature have documented types of attacks that violate aspects of the CIA triad.

Eavesdropping: Also known as sniffing or snooping attacks, is the theft of information transmitted over the network by a computer, smartphone, or other connected devices [44].

Cross-Site Request Forgery (CSRF): Forcing victims to use their victim's authentication token to make an unwanted request [45].

SQL Injection Attack: The attacker enters an SQL query via input data from the client to the application to control or perform administrative operations on the database [46].

Cross-Site Scripting (XSS) attack: Attacker injects HTML code or Client Script on a website to bypass security on the client-side to obtaining sensitive information and inserting malicious applications [45].

Side-channel attack: Attacker takes advantage of leaked information caused by machine or program activity to find a user's key and retrieve data from an encrypted device [47].

Distributed Denial of Service (DDoS): DDoS is a type of attack by flooding internet network traffic on a server, system, or network using several attacker host computers until the target computer is inaccessible [46].

Brute-Force Attack: Attempt to gain access to an account by guessing the username and password used. In launching the attack, the perpetrator uses a trial-and-error method by trying all password combinations to pass the authentication process [48].

Replay Attack: Attack on a security protocol using playback of messages from a different context into the original context, thereby tricking legitimate users into thinking they have completed the protocol being executed [49].

Session Hijacking: The act of taking control of the user's session after the attacker has successfully obtained the session ID authentication stored in cookies so that the attacker takes control of the session the user has during the session [50].

Virtual Machine (VM) Escape: An attempt to exploit security to gain access to the primary hypervisor and virtual machines so that hackers gain access to the top-level virtualization layer running on that host [51].

Unauthorized Access: Type of crime committed by entering/infiltrating a computer network system illegally, without permission, or without the knowledge of the owner of the computer network system which he entered for sabotage, theft of important information such as personal data, and using resources [49].

The aspects of the CIA triad that violated by the above types of attacks are shown in Table 5:

Table 5. Types of Cyberattacks and the Effects on the CIA Triad

Attack Type	The Effects on the CIA Triad			
	Conf.	Integ.	Avail.	Auth.
Eavesdropping	✓	✓	✓	
Cross-Site Request Forgery (CSRF)				✓
SQL Injection Attack	✓	✓		✓
Cross Site Scripting (XSS)	✓			✓
Side-Channel Attack	✓			✓
Distributed Denial of Service (DDoS)			✓	
Brute-Force Attack	✓			✓
Replay Attack				✓
Session Hijacking				✓
Virtual Machine (VM) Escape	✓			✓
Unauthorized Access	✓	✓		

3.6 Critical Success Factors

[52], in the late 1970s, introduced the concept of Critical Success Factors (CSF) as a mechanism used by top management and executive officers to determine information needs [53] [54]. [55] stated that CSF is used to identify or present the main factors that become the focus of attention for the success of an organization. [54] defines CSF as a limited number of areas with satisfactory results that will ensure successful competitive performance for organizations, departments, or individuals [56]. Dickinson defined CSF as a condition, activity, event, or state that requires special attention from management because of its significance [57].

4. DATA ANALYSIS AND FINDINGS

This section provides a discussion of analysis and findings collected from interviews, highlighting ways and means of analyzing interviews and data triangulation methods to ensure the validity and reliability of research results. The last part is to collect the determining factors for the successful implementation of cybersecurity in smart cities as the outcome of this research.

In this study, interviews were conducted to describe the challenges faced by cybersecurity implementation, as well as to identify practical ways to successfully implement cybersecurity in smart cities, especially in Indonesia. Interviews are specifically taken to identify CSFs for the successful implementation of cybersecurity. Interviews were conducted with policymakers and staff involved in cybersecurity in Jakarta smart city. Semi-structured and informal interview styles were chosen because this approach is flexible and allows the researcher to ask new questions during the interview [8][56]. The benefit of semi-structured interviews is that the researcher has control over the obtaining information process, and during the interview, can pursue new instructions [59]. On the other hand, the interviewer can give flexibility to the source so that the interviewer speaks honestly and the interviewer gets in-depth information about the subject discussed.

To maintain validity, and reliability this study used the triangulation method of data sources. Triangulation of data sources is to explore the truth of certain information by using various data sources such as documents, archives, and the results of interviews with more than one subject who is considering to have different points of view. [60] states that data from interviewees are cross-checked with their peers to maintain validity. The validity in this description reflects the postpositivist view of triangulation as a method of increasing the likelihood that one's findings will be accurate and reliable [61].

The research data are collected through interviews and documentary research. During the interview, the interviewees were asked various questions on the same topic to test whether they would give consistent answers. At the same time, interviewees were observed for their tone of speech and body language. This observation of tone of speech and body language was carried out because the interviewee might be afraid to give a sincere answer as the theme of this research touched on the policies of state officials. Therefore, researchers must consider the tone of speech and body language of the interviewees and do not have complete confidence in their words. For example, when interviewers asked about the responsibilities of leaders, some interviewees tended to need more time to think about their answers, and some answered, "these things are the policies of the leaders, and we do not have the authority to judge them." It makes it difficult for researchers to find the truth. Therefore, documentary data used to confirm, complete, and check information from interviewees. Data and information related to cybersecurity implementation collect from various sources such as journals, official documents, and the script of regulations related to cybersecurity. Documentary data helps fill in the missing pieces of sensitive stories from interviews.

The theme for each of the studied factors identified by reading the interview results that transcribe using analytic coding techniques. [62] states that to assist researchers in indexing text segments into specific themes, researchers can use Nvivo as analysis software. Nvivo is a qualitative analysis software. Nvivo (Version 12) has been used to compile and manage data collected from interviews. With Nvivo themes, that emerge from the text are coded and categorized so that researchers can examine possible relationships between themes.

Data analysis using Nvivo software produces three primary nodes, technology, process, and people, each of which has sub-factors. The three primary nodes were identified in the literature review as three factors that emerged as the main concepts in this study.

The research results prove that three main factors determine the success of the implementation of cybersecurity in Indonesia, namely the process factor, the technology factor, and the people factor.

Among the three main factors, there are 15 critical success factors identified from this study, it can see in Table 6.

Table 6. Critical Success Factors that Highly Influence Cybersecurity Implementations.

Main Factor	Critical Success Factors	Number of references
People	Awareness	9
	Habit and Behaviour	13
	Sectoral Ego	4
	Knowlegde	22
	Governance	26
	Leadership Commitment	8
Proces	Laws and Regulation	5

	Policy	7
	Local Wisdom Value	1
	Standarizaton	45
	Cooperation	23
	Funding	3
Technology	Infrastructure	6
	Framework	3
	Firewall	1

Awareness: Awareness in cybersecurity refers to being responsible for security and taking measures to secure systems, devices and networks, and knowing the importance of security. Everyone who is directly involved in the implementation of cybersecurity should have this responsibility. Awareness is a starting point that must have to achieve security goals.

Knowledge: Knowledge is a crucial factor in achieving security goals. With good knowledge, policymakers and implementers in implementing cybersecurity will know the positive and negative impacts that can cause, so that it will increase awareness of cybersecurity in order to avoid cybercrime cases.

Habit and Behavior: A key element of cybersecurity must involve recognizing the importance of human habits and behavior when designing, building, and deploying cybersecurity technology. The habit and behavior refer to the negligence habit of cybersecurity users which can open up opportunities for crime and attacks due to the negligence. Cybersecurity stakeholders must have a strategy to mitigate cybercrime due to user habits and behavior.

Sectoral Ego: Sectoral ego refers to the compliance and responsiveness of the implementer in implementing cybersecurity. It was trigger by the resistance of each individual or group to policies implemented regarding cybersecurity. Sectoral ego has the consequence of a slowdown in cybersecurity implementation.

Governance: Governance refers to the authority of the leadership in giving cybersecurity executives the flexibility to plan and implement cybersecurity. However, cybersecurity implementers still have to comply with applicable laws and regulations. In governance, it is best if each cybersecurity executive unit has a national cyber governance master plan. With the national governance master plan, each cybersecurity implementing unit has a reference for developing security according to the needs of their respective units.

Leadership Commitment: Leadership support and commitment are important and necessary during implementation to provide and allocate adequate resources. Support also motivates the team to work harder on creating new ideas to speed up the process and address obstacles such as resistance to change and funding.

Laws and Regulations: Laws and regulations are other crucial instruments needed in cybersecurity development. These tools can effectively compel individuals or groups to remain compliant in carrying out cybersecurity-related tasks. This device is the main handle of all cybersecurity stakeholders in their respective positions.

Policy: As with laws and regulations, the policy is another crucial instrument needed in cybersecurity development. This instrument complements law and regulation.

Local Wisdom Value: Local wisdom values refer to the availability of resources to support cybersecurity development in an area. These resources include budget management policies, the availability of human resources (cybersecurity professionals), and the availability of cybersecurity supporting peripherals.

Standardization: Standardization refers to the guarantee that the security system used such as hardware, software, and governance will be compatible with other systems that refer to the same standard. One of the standards used in cybersecurity governance is ISO. Standards are the single most important element in achieving cybersecurity integration.

Cooperation: Cooperation with other parties need to respond to cybersecurity incidents quickly, efficiently and effectively, to be able to anticipate cyber-attacks. Cooperation can carry out with other agencies within the same local government, national and international cooperation, cooperation with universities, and cooperation with cybersecurity professionals.

Funding: Cybersecurity initiatives around the world need funds to procure security devices, both software, and hardware. Furthermore, funding is a requirement for the sustainability of cybersecurity implementation. The importance of funding is very crucial in providing excellent service to citizens and ensuring the security of personal data in all transactions in cyberspace.

Infrastructure: In providing security services through the Information and Communication Technology component, which is capable of supporting and enabling the delivery of cyber services consisting of a security infrastructure for server environments, networks, applications, data and content management tools. This security infrastructure is the backbone of any security implementation and a key factor for success.

Framework: Framework in cybersecurity serves as system standards, guidelines, and best practices for managing emerging risks related to security, both digital and physical. Developing a cybersecurity framework should prioritize a flexible, sustainable, and cost-effective approach.

Firewall: The role of a firewall in cybersecurity, especially networks, is to inhibit external threats such as hackers and protect the internal network infrastructure from virus and malware attacks.

5. CONCLUSION AND FUTURE REMARKS

This paper has discussed the determinants of the successful implementation of cybersecurity in smart cities in Indonesia. Four stages have used to identify CSFs for cybersecurity implementation, involving; a) investigating existing models and factors for the success of implementing cybersecurity, b) the preparation process, c) the implementation process and d) the data analysis process. It consists of a detailed literature review of some of the common factors associated with recognized cybersecurity development. Fifteen CSFs concerning the implementation of cybersecurity in smart cities in Indonesia identified, namely factors of knowledge, habit, sectoral ego,

awareness, governance, leadership commitment, laws and regulation, policy, local culture, standardization, cooperation, funding, infrastructure, framework, and the firewall.

Understanding these factors is essential for advancement in academia and practice, for example, to understand what drives the success of

cybersecurity initiatives, to form the basis for deriving performance measures related to cybersecurity development, and to support the design and implementation of shared governance and service structures. Therefore, providing a strong CSF foundation for further research into cybersecurity implementation is extremely important. These fifteen aspects are important to pay attention to and manage to ensure the success of cybersecurity in developing countries.

REFRENCES

[1] Piro G, Cianci I, Grieco LA, Boggia G, Camarda P. Information centric services in smart cities. *J Syst Softw*. 2014;88(1):169-188. doi:10.1016/j.jss.2013.10.029

[2] Allen N. Cybersecurity weaknesses threaten to make smart cities morecostly and dangerous than their analog predecessors. *London Sch Econ*. Published online 2016.

[3] Hadi MDS, Widodo P, Putro RW. Analysis of the Impact of the Covid 19 Pandemic in Indonesia from a Cybersecurity Point of View. *Natly J*. 2020;1(1):1-9.

[4] Wahyono F. Manifestasi program Jakarta smart city melalui sustainable development goals sebagai ambisi pembangunan global. *Jounal Sustain Archit*. Published online 2019:1-15.

[5] Bris A, Lanvin B. IMD World Smart City Index 2019. *Smart City Index*. Published online 2019.

[6] Satispi E, Mufidayati K. The Implementation of The Jakarta Smart City (JSC). In: *Evi Satispi and Kurniasih Mufidayati. In Iapa Proceedings Conference*. ; 2019:192-199.

[7] Abdelghaffar H, Bakry WEM, Duquenoy P. E-government: A new vision for success. In: *In Presentado En European and Mediterranean Conference on Information Systems*. ; 2005.

[8] King N. 21——Using Templates in the Thematic Analysis ofText——. In: *Essential Guide to Qualitative Methods in Organizational Research*. ; 2004:256.

[9] Yin RK. *Case Study Research: Design and Methods (Applied Social Research Methods)*. Sage; 2009.

[10] Bifulco F, Tregua M, Amitrano CC, Anna D. ICT and sustainability in smart cities management. *Int J Public Sect Manag*. 2016;29(2):132-147.

[11] Zurita G, Pino JA, Baloian N. Supporting Smart Community Decision Making for Self-governance with Multiple Views. 2015;2:134-143. doi:10.1007/978-3-319-26401-1

[12] Ziadi AR, Supriyono B, Wijaya AF. The Effectiveness of Information System in Public Complaint Service: An Implementation of E-Government based on Jakarta Smart City Applications. *Glob J Manag Bus Res A Adm Manag*. 2016;16(8):53-57.

[13] Kurnia T. Accelerated Development of Jakarta Smart City. *Reka Ruang*. 2020;3(1):27-35.

[14] Tampubolon L. Indonesian E-Government Ranking (PeGI) and information technology utilization in DKI Jakarta. *urnal Sist Inf*. 2016;8(2):1121-1132.

[15] Wang J, Gupta M, Rao HR. Insider Threats in a Financial Institution: Analysis of Attack-Proneness. *Mis Q*. 2015;39(1):91-112.

[16] Cerrudo C. An emerging US (and world) threat: Cities wide open to cyber attacks. *IOActive*. Published online 2015.

[17] Danuri M, Suharnawi. Trend cyber crime dan teknologi informasi di indonesia. *INFOKAM*. 2018;2:55-64.

[18] Ardiyanti H. Cybersecurity dan tantangan pengembangannya di Indonesia. *Politica*. 2018;5(1):95-110.

[19] Kesswani N, Kumar S. Maintaining Cyber Security: Implications, Cost and Returns. *Proc 2015 ACM SIGMIS Conf Comput People Res - SIGMIS-CPR '15*. Published online 2015:161-164. doi:10.1145/2751957.2751976

[20] Meeuwisse R. *Cybersecurity for Beginners*. Cyber Simplicity Ltd; 2017.

[21] Batteau AW. Creating a culture of enterprise cybersecurity. *Int J Bus Anthropol*. 2011;2(2):36-47.

[22] Klaper D, Hovy E. A taxonomy and a knowledge portal for cybersecurity. *Proc 15th Annu Int Conf Digit Gov Res - dg.o '14*. Published online 2014:79-85. doi:10.1145/2612733.2612759

[23] ISO. Information technology — Security techniques — Guidelines for cybersecurity. *ISO/IEC 27032:2012*. Published online 2012.

[24] Solms R Von, Niekerk J Van. From information security to cyber security. *Comput Secur*. 2013;38:97-102. doi:10.1016/j.cose.2013.04.004

[25] Cavelty MD. Cyber-Terror-Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate. *J Inf Technol Polit*. 2008;4(1):19-36.

[26] Friedman AA, West DM. Privacy and security in cloud computing. *Cent Technol Innov Brookings*. 2010;3:1-13.

[27] Buzan B, Wæver O, Wæver O, De Wilde J. *Security: A New Framework for Analysis*. Lynne Rienner Publishers; 1998.

[28] Oxford University Press. Oxford Online Dictionary. Oxford: Oxford University Press. Published 2021. Accessed April 28, 2021. http://www.oxforddictionaries.com/definition/english/Cybersecurity

[29] Kemmerer RA. Cybersecurity. In: *Proceedings of the 25th IEEE International Conference on Software Engineering*. ; 2003:705-715.

[30] Lewis JA. Cybersecurity and Critical Infrastructure Protection. In: *Washington, DC: Center for Strategic and International Studies*. ; 2006.

[31] Amoroso E. *Cyber Security*. . New Jersey: Silicon Press; 2006.

[32] ITU. Overview of Cybersecurity. Recommendation ITU-T X.1205. *Geneva Int Telecommun Union*. Published online 2008.

[33] Canongia C, Mandarino R. Cybersecurity: The New Challenge of the Information Society. In: *In Crisis Management: Concepts, Methodologies, Tools and Applications*. Hershey, PA: IGI Global; 2014:60-80.

[34] Craigen D, Diakun-Thibault N, Purse R. Defining cybersecurity. *Technol Innov Manag Rev*. 2014;4(10):13-21.

[35] Ten CW, Liu CC, Manimaran G. Vulnerability assessment of cybersecurity for SCADA systems. *IEEE Trans Power Syst*. 2008;23(4):1836-1846.

[36] Elmaghraby AS, Losavio MM. Cyber security challenges in smart cities: Safety, security and privacy. *J Adv Res*. 2014;5(4):491-497. doi:10.1016/j.jare.2014.02.006

[37] Hernández-Ramos JL, Jara AJ, Marin L, Skarmeta AF. Distributed capability-based access Control for the internet of things. *J Internet Serv Inf Secur*. 2013;3(3/4):1-16.

[38] Arora A, Nandkumar A, Telang R. Does information security attack frequency increase with vulnerability disclosure? An empirical analysis. *Inf Syst Front*. 2006;8(5):350-362.

[39] Zhao JJ, Zhao SY. Opportunities and threats: A security assessment of state e-government websites. *Gov Inf Q*. 2010;27(1):49-56.

[40] Debruijn H, Janssen M. Building cybersecurity awareness : The need for evidence-based framing strategies. *Gov Inf Q*. 2017;34(1):1-7. doi:10.1016/j.giq.2017.02.007

[41] Baig ZA, Szewczyk P, Valli C, et al. Future challenges for smart cities: Cyber-security and digital forensics. *Digit Investig*. 2017;22:3-13.

[42] Uma M, Padmavathi G. A survey on various Cyber attacks and their classification. *Int J Netw Secur*. 2013;15(5):390-396.

[43] Berkel AR, Singh PM, van Sinderen MJ. An information security architecture for smart cities. In: *In International Symposium on Business Modeling and Software Design*. Springer, Cham; 2018:167-184.

[44] Levy-Bencheton C, Darra E, Bachlechner D, Friedewald M. Cyber security for smart cities-an architecture model for public transport. In: *The European Union Agency for Network and Information Security, Tech. Rep.* ; 2015.

[45] Aung TM, Oo MM. Defensive Analysis on Web-Application Input Validation for Advanced Persistent Threat (APT) Attack. In: *Fourteenth International Conference On Computer Applications (ICCA 2016)*. ; 2016.

[46] Li Y, Dai W, Ming Z, Qiu M. Privacy protection for preventing data over-collection in smart city. *IEEE Trans Comput*. 2016;65(5):1339-1350.

[47] Seibert J, Okhravi H, Eric S. Information leaks without memory disclosures: remote side channel attacks on diversified code. In: *The 2014 ACM SIGSAC Conf. on Computer and Comm. Security. Scottsdale, Arizona,*. ; 2014:54-65.

[48] Knudsen LR, Robshaw MJB. Brute force attacks. In: *The Block Cipher Companion*. Springer Berlin Heidelberg; 2011:95-108. doi:http://dx.doi.org/10.1007/978-3-642-17342-4 5

[49] Sookhak M, Gani A, Khan MK, Buyya R. Dynamic remote data auditing for securing big data storage in cloud computing. *Inf Sci (Ny)*. 2017;380:101-116.

[50] Bhattasali T, Chaki R, Chaki N. Secure and trusted cloud of things. In: *Proc. Annual IEEE India Conf. (INDICON)*. ; 2013:1-6.

[51] Rehman A, Alqahtani S, Altameem A, Saba T. Virtual machine security challenges: Case studies. *Int'l J Mach Learn Cybern*. 2014;5(5):729-742.

[52] Rockart. Chief executives define their own data needs. *Harv Bus Rev*. 1979;57:81-93.

[53] Khandelwal VK, Ferguson JR. Critical success factors (CSFs) and the growth of IT in selected geographic regions. In: *Proceedings of the 32nd Annual Hawaii International Conference*. IEEE; 1999:13-pp.

[54] Rockart JF. The changing role of the information systems executive: a critical success factors perspective. *Massachusetts Inst Technol*. Published online 1982.

[55] Kahreh MS, Mirmehdi SM, Eram A. Investigating the critical success factors of corporate social responsibility implementation: evidence from the Iranian banking sector. *Corp Gov*. 2013;13(2):184-197.

[56] Jamil MR, Ahmad N. Present status and critical success factors of e-Commerce in Bangladesh. In: *Computers and Information Technology, 2009. ICCIT'09. 12th International Conference*. IEEE; 2009:632-637.

[57] Duquenoy P, Bakry WEM, Abdeghaffar H. E-government: a new vision for success. In: *European and Mediterranean Conference on Information Systems*. ; 2005.

[58] Baxter P, Jack S. The Qualitative Report Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers. *Qual reportualitative Rep*. 2008;13(2):544-559. doi:citeulike-article-id:6670384

[59] Bernard HR. *Research Methods in Anthropology*. Rowman Altamira; 2011.

[60] Downie C. Three ways to understand state actors in international negotiations: climate change in the Clinton years (1993–2000). *Glob Environ Polit*. 2013;13(4):22-40.

[61] Love PED HG, Li H. Triangulation in construction management research. *Eng Constr Archit Manag*. 2002;9(4):294-303.

[62] Azeem M, Salfi NA, Dogar AH. Usage of NVivo software for qualitative data analysis. *Acad Res Int*. 2010;2(1):262-266.