Cybersecurity project implementation for resources protection: a case study of the National Narcotics Board

A C Nugrah¹, A N Hidayanto¹, H S Indriany², H Kurniati², B M A Firdaus² and Bastara²
¹Faculty of Computer Science, Universitas Indonesia, Indonesia
²ICT Department of National Narcotics Board, East Jakarta, Indonesia

Abstract. Cybersecurity is currently being used by government organizations in protecting their resources such as data and assets as well as avoiding catastrophic pollution and the failure of key infrastructure that can harm human health and environment. The increasingly modus operandi of modern drug crime syndicates which utilizing technology to attack the network of the National Narcotics Board (NNB) is a threat and vulnerability for NNB, so NNB must make efforts to mitigate the risk. Research on the implementation of cybersecurity projects at the National Narcotics Board aims to explore information related to the implementation of cybersecurity projects in securing and defending data and information networks at NNB. The research method used is a descriptive approach with qualitative methods through semi-structured interviews and observation. This cybersecurity project provides benefits for data and information protection at NNB, through a cybersecurity monitoring system assisting NNB in monitoring cyber traffic conditions in real-time. From this study, it was found that the factors influencing the implementation of cybersecurity projects that were mapped to critical success factors for information technology projects, namely involvement and effective communication, capability and motivation of the team, capability, and leadership of the project manager, requirements management, clear project objectives, and top-level management support levels.

1. Introduction
Along with the development of technology and information flow, efforts to protect information from cyber-attack are required. Cybersecurity can protect data and information which are valuable assets of an organization as an effort in cyber defence.

Based on a data survey from APJII (Association of Indonesian Internet Service Providers), internet users in the period of 2019 to the second quarter of 2020, 73.7% or 196.71 million people were internet users out of 266.91 million Indonesians. From this data, we can see that the penetration of internet users in Indonesia is increasing every year [1].

Based on the 2019 ID-SIRTII/CC internet traffic data, there are 10 largest attack classifications, namely: malware/PoS malware (39%), account hijacking (17%), unknown (12%), targeted attack (11%), vulnerability (5%), malicious script injection (4%), malicious spam (2%), DoS/DDoS (2%), fake accounts/pages (1%), misconfiguration (1%), and others (6%) [2].

Cybercrime can lead to the loss of control of vital equipment and warning systems, as well as catastrophic spills, waste discharges, and air pollutants that can harm human health and the environment. As a result, a breach of cybersecurity could result in catastrophic pollution and the failure of key
infrastructure. Cybercrime has also an impact on the economic sector, based on data from 2017, Norton cybersecurity, insight report global results, from 978 million adults in 20 countries, one of which is Indonesia with a total of 59.45 million adults who are perpetrators of cybercrime. The total loss of consumers who are victims of cybercrime globally, Indonesia reaches $ 3.2 billion [3].

From the information data on cyber honeynet project attacks by the National Cyber and Crypto Agency (NCCA) as shown in Figure 1, it can be seen that Indonesia is the second-highest attack target after India.

![Figure 1. Honeypot Cyber Attack Information](image)

The National Narcotics Board (NNB) is a government board in charge of the Prevention of Eradication of Narcotics Abuse and Illicit Trafficking [4]. According to research conducted by NNB, it is known that the prevalence of drug abusers in Indonesia is 1.80% or equivalent to 3.42 million people [5]. With a large number of drug abusers in Indonesia, NNB has declared war on drugs. The increasing modus operandi of modern drug crime syndicates, by utilizing technology to attack the NNB network, is a threat and vulnerability for NNB, so NNB must make efforts to mitigate risk. This study aims to determine the process of implementing a cybersecurity project in securing and defending data and information networks in NNB.

In previous studies, Creado and Ramteke [6] analysed and recommended active cyber defence strategies and techniques that can be applied by organizations in the financial sector is to secure their cyber assets and space [7]. Analyses traffic on the internet through social networks using a set of general concepts of similarity, correlation, and collective indication [8]. The UK's Active Cyber Défense (ACD) program has been a key aspect of the National Cyber Security Centre’s (NCSC) work on improving public sector cyber security by objectively reducing the threat of cybercrime to government agencies and service users.

This research is new research on cyber active defence strategy in the war on drugs. Discussions related to cybersecurity in the Indonesian government have not been discussed much in previous studies. Furthermore, the question in this research is how to implement cybersecurity projects and what lessons can be learned? This research is structured as follows: part I is the introduction. Part II provides a literature review on this topic. Part III describes the research methodology used for this study. Part IV results and discussion. Part V conclusion and future works obtained from the research.

2. Literature Review

2.1. Cybersecurity

Cybersecurity is defined as a combination of the processes involved in storing individual and organizational data both online and offline [9]. Cybersecurity is also the process and techniques involved...
in protecting sensitive data, computer systems, networks, and software applications from cyber-attacks [10].

Theoretical and empirical insights note that cybersecurity awareness is a topic of particular interest in cybersecurity [11]. Cybersecurity systems, which protect networks and computers against cyber-attacks, are becoming common due to increasing threats and government regulation, the enormous amount of data gathered by cyber-security systems poses a serious threat to the privacy of the people protected by those systems [12].

2.2. Cyber Defence
Cyber defence is an effort to overcome cyber-attacks that disrupt the implementation of national defence [13]. It can also be defined as the use of digital tools to defend computer systems and networks from cyber-attacks and malicious intrusions [14]. Active Cyber Defence (ACD) is a way/technique to achieve this.

2.3. Cybersecurity within Indonesian Government
To anticipate cyber security, in Indonesia, the National Cyber and Crypto Agency (NCCA) through the Directorate of Countermeasures and Recovery, the Deputy for Countermeasures and Recovery of the BSSN formed the Government - Computer Security Incident Response Team Indonesia (Gov-CSIRT) to combat the existence of cybersecurity threats and cyber-attacks, by collaborating and cooperating between ministries or government agencies. The main goal of CSIRT is to minimize and control the damage, provide response assistance and effective recovery, and help to prevent reoccurrence [15]. NNB has also formed a CSIRT team consisting of 25 team members [16]. The NNB CSIRT team is the initiator of the cybersecurity project at NNB which is motivated by the findings from BSSN on the number of cyber-attacks that enter the network system at NNB.

2.4. Success Factor
Critical Success Factor (CSF) is an element that must be implemented properly so that the activities of a project can run successfully. The success of a project can be seen from whether it is following the desired specifications, costs, and time. CSF is a critical success factor so it needs to be known so that companies can take the right steps and ensure competitive work. CSF analysis is concerned with the identification of areas where something must be right if the company is going to be successful [17].

3. Materials and Method
This study uses a descriptive approach with a qualitative case study method at NNB. Qualitative research is a study whose research results are not obtained through statistical procedures or other quantification methods [18]. The methodologies used in this study include:

3.1. Literature Study
The literature study is to learn about cyber security and analyse the object of research, the National Narcotics Board in more depth.

3.2. Data Collection
Primary data were collected from the results of semi-structured interviews and observations. In this study, interviews were conducted with resource persons involving two functional positions of computer system administrators in the field of Information and Communication Technology as well as a person in charge of the cybersecurity project and one Project Manager from the project-winning vendor. In addition, observations of the environment were also carried out to see the processes that have been running up to now. The interview and observation processes were carried out for 3 days. Secondary data is data used as additional material/reference collected from literature studies related to previous research, cyber-security project documents to study processes in cybersecurity project implementation.
3.3. Data analysis
The analytical method used is thematic analysis, which is one way to analyse data to identify patterns and find themes through the data that has been collected. There are six stages carried out for thematic analysis, namely: introduction to data, coding, finding themes, reviewing themes, defining and naming themes, and writing [19]. In this study, thematic analysis was carried out by recording, transcription, coding, and writing interviews. Analyse the results of interviews, observations, and literature studies to obtain information about the implementation of cybersecurity projects. The analysis carried out includes an analysis of the situation before the cybersecurity project, implementation, post-implementation, challenges, and success factors in the cybersecurity project at NNB.

3.4. Conclusions and suggestions
The overall results of the analysis obtained from the results of the research carried out will be drawn into a conclusion. Furthermore, suggestions or recommendations will be given to NNB regarding matters that can be improved in the future so that cybersecurity implementation will be better in the future.

4. Result and Discussion
There are a series of processes in the implementation of cybersecurity projects, starting from the planning stage to the handover stage [20], as shown in Figure 2.

![Figure 2. Conceptual Model Stages of Government Goods/Services Procurement](image)

In this study, the discussion focuses on the contract implementation process which is the main activity of a series of processes in a project in the Government.

4.1. Assessment Results for Current Condition
After signing the work contract between NNB and the winning vendor, the first step in implementing the cybersecurity project is to conduct an assessment of current conditions. Based on the results of interviews with informants, it is known that the current state or condition is carried out with an assessment, which aims to find and detect errors or weaknesses in the NNB network. Cyber security and performance assessments are carried out based on 5 tiers which refer to standardization documents issued by international standardization institutions such as ICANN, NIST, W3C, and IETF [21]. The results of the assessment of the 5 tiers of the basic foundations of cyber security are as in table 1.

4.2. Result
From the results of the assessment carried out, there are several shortcomings and errors in the infrastructure and network, including IPv6 has not been implemented, there is no DNS protection, connections to the NNB website have not used a secure protocol (HTTPS), have not implemented Content Security Policy for security from attacks such as clickjacking, there is no certificate validation on NNB email addresses, NNB web performance is still slow due to script errors that do not follow reference standards, IP and network traffic arrangements are not good, there is no server and client zone separation, lack of network protection functions, the existence of a public IP directly to the server zone which is very vulnerable from outside attacks, wasteful use of client IP.
Table 1. Preliminary Assessment Results

| Cyber Security Category | Assessor | Result            |
|-------------------------|----------|-------------------|
| Availability of Modern Internet Protocol (IPv6) and Application of Latest Technology | Mythic Beasts, IPv6 Validator, IPv6 Survey | Not Available Grade: 6% |
| Domain Name Security | Verisign Labs | Not Available Grade: F |
| Cryptographic Security and Standardization | Qualys, High-Tech Bridge | Not Available Grade: F |
| Information System Infrastructure Security | Sophos, High-Tech Bridge, Internet NL, Netcraft | Not Available Grade: F |
| Email Transaction Security | Internet NL, Vircom, European Commission, Global Cyber Alliance, Dane SMTP | 63% |

4.3. Recommendations

It is necessary to improve the security of the application system and network system. In the system application, it is necessary to adopt the use of TLS/SSL which ensures the privacy and integrity of the communication of network devices, it is necessary to take steps to secure the domain, it is necessary to implement a cryptographic system in NNB applications, it is necessary to implement the use of IPv6 in the NNB environment, it is necessary to make improvements to the script on applications that do not meet application security standards, need to integrate applications that run with data and information network security. Meanwhile, in the network system, it is necessary to adjust the upstream/internet line for data and information network security, it is necessary to design the topology and architecture of the data and information network, to separate data access points for public services and for internal purposes, to rearrange the distribution of the local IP network and the DMZ network, to improve security and efficiency, and need to do network cable and data centre rejuvenation.

4.4. Implementation Plan

This cybersecurity project was implemented over 80 days with an 8-person vendor team [21]. After the assessment is carried out, based on the results of the improvement recommendations, there are three stages in the implementation of the cybersecurity project, which begin with the implementation preparation stage, the implementation stage, and the implementation stage testing results.

4.4.1 Preparing. At this stage, identification of the network architecture that has been running is carried out, identification of systems that are running and integrated with network infrastructure, identification of IP and ASN (Autonomous System Number), identification of all network-based devices used, identification of domain systems managed by NNB, identification of application servers used by NNB, and identification of the cyber defence system currently used by NNB.

4.4.2 Implementation. At this stage, installation is carried out, among others, by installing hardware for data and information network security, installing and configuring firewall systems and monitoring systems, managing network traffic by dividing into three zones (primary zone, military zone, internal zone), and implement IPv6.

4.4.3 Implementation result test. After the implementation of the security is carried out, it is necessary to carry out a cybersecurity assessment again to test the results of the implementation of the cybersecurity project. The final results after implementing cybersecurity are as in table 2.
### Table 2. Assessment Results After Cybersecurity Implementation

| Cyber Security Category                                      | Assessor                                                                 | Result          |
|-------------------------------------------------------------|---------------------------------------------------------------------------|-----------------|
| Availability of Modern Internet Protocol (IPv6) and Application of Latest Technology | Mythic Beasts, IPv6 Validator, IPv6 Survey                                | Available       |
|                                                             |                                                                           | Grade: 100%     |
| Domain Name Security                                        | Verisign Labs                                                             | Available       |
|                                                             |                                                                           | Grade: A        |
| Cryptographic Security and Standardization                  | Qualys, High-Tech Bridge                                                 | Available       |
|                                                             |                                                                           | Grade: A+       |
| Information System Infrastructure Security                  | Sophos, High-Tech Bridge, Internet NL, Netcraft                          | Available       |
|                                                             |                                                                           | Grade: A+       |
| Email Transaction Security                                 | Internet NL, Vircom, European Commission, Global Cyber Alliance, Dane SMTP | 98%             |

After project implementation, in conducting cybersecurity monitoring, you can use systems as support in monitoring cyber security activities, including the Network Security System Dashboard, Network Management System, Attack Maps, Cyberthreat Sensor, and IP Address Management System, as shown in Figure 3.
4.5. Lesson Learned
Overall, the implementation of the cybersecurity project was declared successful because it was timely, cost-effective, and efficient. Several success factors that can be taken from cybersecurity implementation projects can be mapped against critical success factors for information technology projects [22]. Based on the results of interviews with Project Managers and NNB Young Expert Computer Institutions, table 3 are CSFs that can be mapped based on success criteria, namely scope, time, cost, quality, and user satisfaction.

Table 3. Assessment Results After Cybersecurity Implementation

| Factor                        | Explanation                                                                 | Interview Quotes                                                                 |
|-------------------------------|-----------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| Customer involvement and      | Good communication between the NNB in this case the ICT team with the PT. XYZ is very influential on the success of the project. The cybersecurity project implementation team coordinates well with each other by utilizing time effectively and efficiently. | “…coincidentally, they visit here every day, coordinate every day, build good communication between us, the NNB team, and the development team, so that any problems can be resolved quickly…” CA1 |
| effective communication       | Supported by a team that is capable and experienced in the field of cybersecurity. | “…our team is all certified and experienced because we are a company engaged in security services that are also |
| Capability and motivation of  |                                                                                            |                                                                                  |
| the team                      |                                                                                            |                                                                                  |
The role of the Project Manager (PM) is very influential, considering that this project only lasts 80 days with a scope of work that quite a lot requires a PM who is strong and experienced in implementing cybersecurity projects.

Requirement management
With a fairly short project execution time, an analysis process is needed on the tasks that will be the main priority, and adjustments are needed if there are changes in needs when the project is running.

Clear project objectives
The project objectives are clear and in detail described in the scope of work in the term of reference (TOR) document.

Top-level management support and organizational culture
Top-level management support in the form of policies, setting strategic goals, planning, directing, managing, and building organizational culture helps the success of this project.

The successful implementation of this cybersecurity project, in general, has also fulfilled the PMBOK Knowledge Area, namely integration, scope, schedule, cost, quality, resource, communications, risk, procurement, and stakeholders [23].

During the implementation process, there were also challenges and obstacles faced, however, these challenges and constraints could be overcome. The Project Manager said that the obstacles were, among others, in terms of the unstable electricity infrastructure and the applications being developed did not refer to safety standards, while the challenge was the relatively short implementation time of 80 days with a large scope of work.

### 5. Conclusion

#### 5.1. Conclusion

The implementation of cybersecurity projects at NNB is driven by the need for NNB to improve cyber security. The project was declared successful on time, the vendor-provided post-implementation services, and the system rarely experienced any problems. The implementation of cybersecurity, making the National Narcotics Board one of the nine government institutions of the Republic of Indonesia that have successfully implemented IPv6. The following are the results of the cybersecurity project:

1. System Network: IPv6 implementation, DNS protection, SSL certificate, content security policy, IP and network traffic arrangement, server and client zone separation, network security system, efficient use of Public IP, network grouping based on function, monitoring system and attack detection, IP address management system, security in email and hosting systems.
2. System Application: has adopted the use of TLS/SSL which ensures the privacy and integrity of network device communications and has taken steps to secure the domain by configuring digital signatures in DNS.

Some factors influence the successful implementation of cybersecurity projects that are mapped to critical success factors for information technology projects, namely involvement and effective communication, capability and motivation of the team, capability, and leadership of the project manager, requirements management, clear project objectives, and top-level management support.

5.2. Implication
The main contribution, as well as the implications for the organization, is that this research maps the success factors of a project, in this case, a cybersecurity project. From the success factors in the implementation of cyber security projects, it can be used as a guide in the implementation of other IT projects. While the theoretical implication is that in the field of information technology, you can see new developments in cyber security technology.

5.3. Future Work
As future work, among others, technical standardization is necessary as a guide in future development, interconnection development of the Central NNB with NNB Province and NNB District, and standardization of application development documents that refer to security standards.

References
[1] Anonymous 2020 Internet Survey Report APJII 2019-2020 (Jakarta: Asosiasi Penyelenggara Jasa Internet Indonesia)
[2] Anonymous 2020 National Internet Traffic Monitoring System Report (Jakarta: Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center)
[3] Anonymous 2018 2017 Norton Cyber Security Insights Report Global Results (Amerika: Symantec)
[4] Anonymous 2009 Law of the Republic of Indonesia Number 35 of 2009 concerning Narcotics
[5] Anonymous 2020 Drug Abuse Prevalence Survey 2019
[6] Creado Y and Ramteke V 2020 J. Financ. Crime 27 771–780
[7] Coulter R, Han Q L, Pan L, Zhang J and Xiang Y 2020 Trans. Cybern. 50 3081–3093
[8] Stevens T, O’Brien K, Overill R, Wilkinson B, Pildegovičs T and Hill S 2019 UK Active Cyber Defence January 1–40
[9] Bakht H 2020 Cyber Security (Seattle: Kindle Publisher)
[10] Kalu C O, Chidi-Kalu E, Okidi I A A and Usiedo B A 2020 Libr. Philos. Pract. p 1
[11] Kovacevic A, Putnik N and Toskovic O 2020 IEEE Access 8 125140–125148
[12] Toch E, Bettini C, Shmueli E, Radaelli L, Lanzi A, Riboni D, Lepri B 2018 ACM Comput. Surv. 51 1–27
[13] Anonymous 2014 Minister of Defence Regulation No. 82 of 2014 concerning Cyber Defence (Jakarta: Kementrian pertahanan Republik Indonesia)
[14] Dewar R 2017 Active Cyber Defence (Zurich: Center for Security Studies)
[15] Anonymous 2018 Government CSIRT Indonesia (Jakarta: Badan Ciber dan Sandi Negara)
[16] Anonymous 2019 Computer Security Incident Response NNB Team (NNB - CSIRT)
[17] Olson D L 2004 Introduction to Information System Project Management (McGraw-Hill)
[18] Setiawan J A A 2018 Qualitative Research Methodology (Jakarta: CV Jejak)
[19] Braun V and Clarke V 2006 Qual. Res. Psychol. 3 77–101
[20] Anonymous 2018 Presidential Regulation of the Republic of Indonesia Number 16 of 2018 concerning Government Procurement of Goods/Services
[21] Anonymous 2019 Work Implementation Report “Data and Information Network Security” (European Union Agency for Network and Information Security)
[22] Gumay L A Purwandari B Raharjo T Wahyudi A and Purwaningsih M 2020 Int. Conf. Proceeding Ser.108–112
[23] Anonymous 2017 Guide to the Project Management Body of Knowledge (PMBOK Guide) 6th. Edition