BEST
Journal of Applied Electrical & Science Technology – University of PGRI Adi Buana Surabaya
p-ISSN 2715-2871
e-ISSN 2714-5247

Cybersecurity Measures For Election Information Systems : Sistem Rekapitulasi Suara Pemilu 2024 (siRekap)

Dwi Hastuti
Electrical Engineering
University of PGRI Adi Buana
Surabaya, Indonesia
dwi.hastuti@unipasby.ac.id

Sagita Rochman
Electrical Engineering
University of PGRI Adi Buana
Surabaya, Indonesia
sagitarochman@unipasby.ac.id

Rasyida Shabihah Zukro Aini
Electrical Engineering
University of PGRI Adi Buana
Surabaya, Indonesia
rasyida@unipasby.ac.id

Abstract— All election data in Indonesia is processed and stored by the General Election Commission (Komisi Pemilihan Umum Republik Indonesia-KPU) using the Election Recapitulation Information System (SiRekap). The SiRekap system complies with the relevant laws, and all of its data is handled and kept in an Indonesian data center. Elections are vulnerable to a spectrum of technological threats that range from traditional cybersecurity concerns, such as hacking and data breaches, to more sophisticated forms of manipulation, such as deepfakes and AI-generated disinformation. Threat actors may exploit vulnerabilities in election infrastructure, targeting electronic voting systems and voter databases. Preventive cybersecurity measures are essential for protecting elections from ever-changing cyberattacks, such as : shared responsibility for cybersecurity, using cybersecurity to gain an edge, the legal and regulatory need for cybersecurity, best practices for cybersecurity, real-world cybersecurity examples, the ideal choice for companies and institutions. The government is essential role to ensuring cybersecurity. Improved cybersecurity would be especially beneficial in averting leaks and hacks. At a fair price, election systems themselves may be significantly strengthened in terms of security.

Keywords— Cybersecurity, Election Information Systems (SiRekap), Role of Governments.

I. INTRODUCTION

A voting system, often known as an election system, is a set of regulations that specify how elections and referendums are held and how their outcomes are decided. These rules control every part of the voting process, including when elections are held, who can run for office and vote, how ballots are marked and cast, counted, and translated into election results, limitations on campaign spending, and other factors that could affect the result. Since 1955, elections have been held in Indonesia. The six principles of direct, general, free, confidential, honest, and fair govern Indonesian election procedure. These ideas are condensed and widely disseminated as "Luber-jurdil". The New Order government began implementing the first four "Luber" principles after the 1971 election.

A platform or tool for organizing and storing election-related data is called an electoral information system. Voter registration, ballot production, vote counting, and result posting are only a few of the functions that it may have. The SiRekap system aims to improve public accountability for the election results by serving as a simple publication assistance and recapitulation tool. As the foundation for tiered determination and the basis for the outcomes of the vote counting, manual recapitulation on a tiered basis is still used. An overview of The SiRekap can be seen in FIGURE1 and FIGURE2.

FIGURE 1. Overview of The SiRekap

All election data in Indonesia is processed and stored by the General Election Commission (KPU) using the Election Recapitulation Information System (SiRekap). The SiRekap system complies with the relevant laws, and all of its data is handled and kept in an Indonesian data center. Since February 14, 2024, the system has been disrupted by DDoS (distributed denial of service) interference. The Commission persisted in addressing the disruption with the help of the cyber task force team. February 15–22 was the scheduled date for the KPU recapitulation; districts were scheduled for February 15–2 March 2024; cities and districts for February 17–5 March 2024; provinces were scheduled

p-ISSN 2715-2871
e-ISSN 2714-5247

for February 19–10 March 2024; and the national was scheduled for February 22–20 March 2024. The general public can see the proceedings of the open plenary meeting where the recapitulation and determination of the vote count results are conducted.

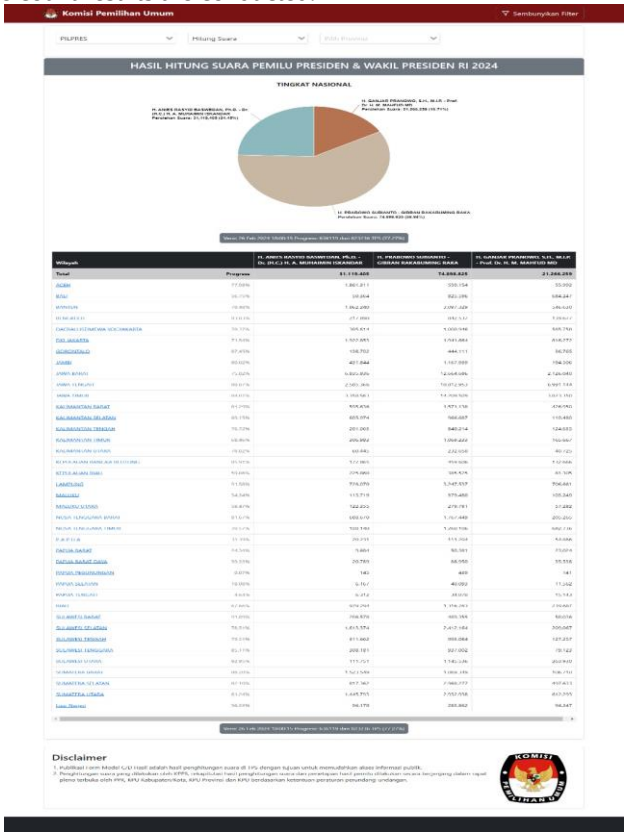


FIGURE 2. Overview of The SiRekap

Any technique, precaution, or method for averting cyberattacks or lessening their effects is referred to as cybersecurity. Its goal is to defend against a variety of threats, from basic computer viruses to complex and expensive ransomware assaults, to people's and companies' systems, apps, computing devices, and sensitive data. An essential component of Indonesia's electoral infrastructure is the SiRekap system, which is employed by the General Election Commission (Komisi Pemilihan Umum Republik Indonesia - KPU). All electoral data is processed and stored by it, and its security is crucial. The government is essential role to ensuring cybersecurity. Improved cybersecurity would be especially beneficial in averting leaks and hacks. At a fair price, election systems themselves may be significantly strengthened in terms of security. Cybersecurity is seen as a high priority by many enterprises. Every day, there is a greater necessity to put in place efficient cybersecurity systems. Cybercriminals are always coming up with more advanced ways to carry out assaults [1]. In order to make sure that an organization is adhering to its cybersecurity policies and strategy, cybersecurity standards—important components of IT governance—are examined [2]. Thus, a business can translate its cybersecurity policy into quantifiable actions by depending on cybersecurity standards. The functional and assurance measures that must be completed to accomplish the organization's cybersecurity goals are made clear by cybersecurity standards [3]. Implementing cybersecurity standards may seem expensive for a company, but the organization will benefit more from the increased confidence and trust it fosters [4]. As per the information acquired on May 2, 2024, from www.standards.org.au, standards are papers that specify specifications, norms, and procedures with the goal of guaranteeing the safety, uniformity, and dependability of goods, services, and systems. Furthermore, according to the definition given by the ISO/IEC, standards are papers or guidelines that are created based on a general consensus and approved by a legal body. They serve as models, samples, or guidelines that aid in achieving the best outcomes possible in a specific setting [5]. In addition to practically satisfying user requests, a standard also takes into account resource and technological restrictions and satisfies verification criteria [6].

Cybersecurity standards are a set of procedures or technical techniques that assist enterprises in protecting their online environment [7]. Beyond written words, numbers, and images, information has value in other forms as well. Intangible types of information include knowledge, concepts, ideas, and brands. Information and other related assets need to be protected from several types of risks in today's interconnected environment, whether they are intentional, unintentional, or natural [8]. Information security is achieved by applying appropriate control measures, such as laws, regulations, procedures, protocols, organizational structure, and the functions of blind and seeing perangkats. In order to achieve these specific business and safety goals, organizations must define, implement, maintain, enhance, and expand this control as needed [8]. The extent of the financial loss, the related legal and regulatory requirements placed on the affected company, and a thorough account of what happened. Users can investigate the statistical characteristics of the resulting losses, which should be taken into account in capital consideration, and determine the factors that lead to risk occurrence thanks to the comprehensive range of variables that are recorded [9]. Learn more about how a successful external attack could impact the entire sector in the event that it discloses private financial data. Their conclusion confirms how important post-incident controls are [10].

I. METHODS

Cybersecurity is becoming a major concern for everyone in the modern digital world, from people to companies and organizations. The frequency and sophistication of cyber threats are rising, and a cyber strike can have disastrous results. Since businesses and organizations are in charge of safeguarding both their own and their clients' and customers' data, they have a crucial role to play in cybersecurity. This section will discuss the role that corporations and organizations play

p-ISSN 2715-2871
e-ISSN 2714-5247

in cybersecurity and how they may help to protect our digital environment.[8]

1. Shared Responsibility for Cybersecurity.
2. Using Cybersecurity to Gain an Edge.
3. The Legal and Regulatory Need for Cybersecurity.
4. Best Practices for Cybersecurity.
5. Real-World Cybersecurity Examples.
6. The Ideal Choice for Companies and Institutions.

An overview of the method can be seen in FIGURE3.

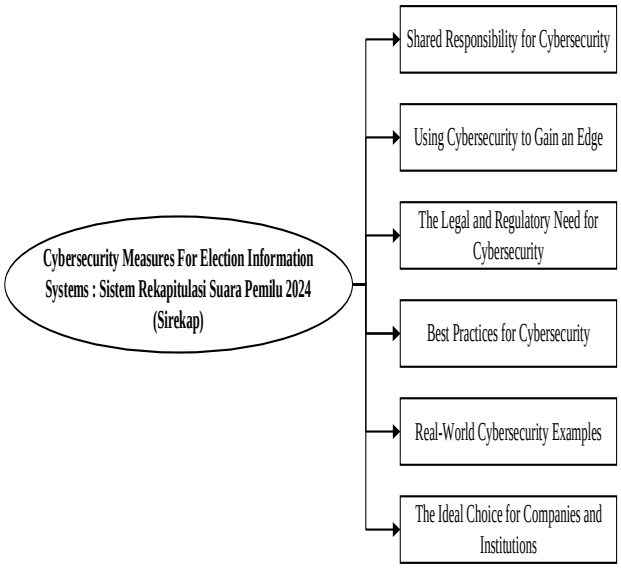


FIGURE 3. Overview of the Method

II. RESULTS AND DISCUSSION

The results section of this study are:

1. Shared Responsibility for Cybersecurity.

One of the most important realizations regarding cybersecurity is that it is a shared duty. Businesses and organizations need more than just government agencies and cybersecurity professionals to keep them safe from online dangers. To safeguard their systems, data, and networks, The General Election Commission (Komisi Pemilihan Umum Republik Indonesia - KPU) need to be proactive. This entails putting in place strong security procedures, training staff members on cybersecurity best practices, and routinely testing and upgrading security safeguards.

2. Using Cybersecurity to Gain an Edge.

Today, having a strong cybersecurity defense is a competitive advantage. Consumers and clients are more inclined to do business with organizations that have a solid cybersecurity image since they are becoming more worried about the protection of their financial, data and personal information. By making cybersecurity investments, The General Election Commission (Komisi Pemilihan Umum Republik Indonesia - KPU) may safeguard their reputation.

3. The Legal and Regulatory Need for Cybersecurity.

Cybersecurity is not just a competitive advantage and a shared duty, but it also has legal and regulatory requirements. Businesses and organizations are required by law in many countries to secure the financial and personal data of their clients and consumers. If The General Election Commission (Komisi Pemilihan Umum Republik Indonesia - KPU) violates these rules, there may be severe penalties, legal repercussions, and reputational harm.

4. Best Practices for Cybersecurity.

The General Election Commission (Komisi Pemilihan Umum Republik Indonesia - KPU) should adhere to cybersecurity experts' advised best practices to make sure they are performing their part in the field. Among them are:

- Using multi-factor authentication and creating strong passwords
- Consistently applying security updates and software updates
- Protecting networks with encryption and firewalls
- Carrying out routine risk assessments and security audits
- Informing staff members about cybersecurity best practices
- Developing an incident response strategy for potential cyberattacks

5. Real-World Cybersecurity Examples.

Numerous instances exist of companies and institutions that have effectively employed cybersecurity protocols to safeguard both their clientele and assets. For instance, making significant investments in cybersecurity and creating cutting-edge security tools and processes in order to safeguard their The General Election Commission (Komisi Pemilihan Umum Republik Indonesia - KPU) networks and data.

6. The Ideal Choice for Companies and Institutions.

When it comes to cybersecurity, the best course of action for The General Election Commission (Komisi Pemilihan Umum Republik Indonesia - KPU) is to have a thorough and proactive strategy. This include making significant investments in strong security measures, training staff members on cybersecurity best practices, testing and upgrading security procedures on a regular basis, and fostering a security-aware culture. Organizations can secure their own data, play their part in cybersecurity, and help to keep safe by doing this.

Cybersecurity is more important than ever as technology becomes more and more integrated into our daily lives. Given the surge in cyberattacks, it is critical that the government actively participate in safeguarding the security and safety of our digital environment. This section will examine the role that the government plays in cybersecurity and the several measures that they may protect our digital environment.

1. Creating guidelines and rules for cybersecurity.

Creating and enforcing laws and regulations to combat the escalating risks in the digital sphere is one of the government's primary responsibilities in cybersecurity.

p-ISSN 2715-2871
e-ISSN 2714-5247

These guidelines may include rules requiring businesses to disclose cyber events or legislation pertaining to data protection. The government can also collaborate with businesses in the private sector to create cybersecurity best practices. For instance, both public and private entities can make use of the cybersecurity architecture for critical infrastructure that NIST, the National Institute of Standards and Technology, has created.

2. Making research and development investments in cybersecurity.

Investing in research and development to advance cybersecurity procedures and technology is one of the government's other major roles in the field. This may entail providing financing for studies on cutting-edge technologies that improve cybersecurity, such blockchain and artificial intelligence. Furthermore, the government may support groups developing cybersecurity breakthroughs with funding and other resources.

3. Working Together with Other Nations and Organizations

Since cybersecurity is a worldwide issue, it is critical that the government work with other nations and organizations to find solutions. This may entail exchanging threat intelligence, organizing the handling of cyberattacks, and creating global cybersecurity standards. For instance, the EU-US privacy shield, which governs the exchange of personal data between the two areas, was developed in collaboration between the US and the EU.

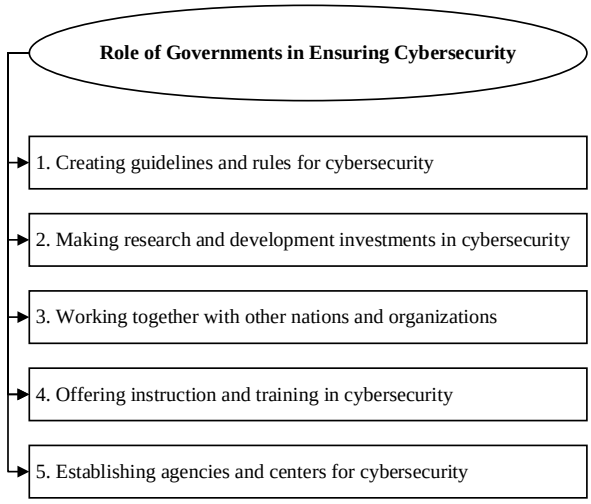
4. Offering instruction and training in cybersecurity

The foundation of every effective cybersecurity plan is education and training. The government may help people and businesses learn how to defend themselves against cyberattacks by offering education and training. This may entail creating campaigns to raise public awareness of cybersecurity issues, educating government personnel, and assisting with cybersecurity education initiatives at universities and colleges.

5. Establishing Agencies and Centers for Cybersecurity

Lastly, organizations and centers for cybersecurity can be established by the government to focus on countering cyberthreats. These facilities can act as a focal point for incident response, threat intelligence exchange, and cybersecurity research and development. The Cybersecurity and Infrastructure Security Agency (CISA) of the United States, for instance, is in charge of defending the country's vital infrastructure against cyberattacks.

The government is essential to ensuring cybersecurity. The government may assist in defending people and companies from cyber dangers by building cybersecurity institutes and agencies, investing in research and development, partnering with other nations and organizations, educating and training people, and implementing legislation and regulations. It is imperative that the government maintains its focus on cybersecurity and actively participates in protecting our digital environment.



III. CONCLUSION

Preventive cybersecurity measures are essential for protecting elections from ever-changing cyberattacks. Election systems can drastically lower the danger of cyberattacks by foreseeing possible weaknesses and remaining one step ahead of hostile actors. This entails constant observation, frequent security assessments, and the application of cutting-edge technology to identify and neutralize such risks before they jeopardize the integrity of election procedures. By taking a proactive stance, election systems are protected against new cyber threats and enhance the overall resilience of the electoral infrastructure.

IV. REFERENCES

[1] G. Mutune, Top Cybersecurity Frameworks, Jul. 2023,[online]Available:https://cyberexperts.com/cybersecurity-frameworks/#2_NIST_Cybersecurity_Framework3

[2] Baron, J.; Contreras, J.; Husovec, M.; Thumm, N, “Making the Rules. The Governance of Standard Development Organizations and their Policies on Intellectual Property Rights,” Publications Office of the European Union: Luxembourg, 2019

[3] H. Taherdoost, "Understanding cybersecurity frameworks and information security standards—A review and comprehensive overview", Electronics, vol. 11, no. 14, pp. 2181, Jul. 2022.

[4] Fumy, W, “IT Security Standardisation,” Netw. Secur, 6-11, 2004.

[5] ISO. ISO/IEC Directives; ISO/IEC: Washington, DC, USA, 2009.

[6] Syafrizal, M.; Selamat, S.R.; Zakaria, N.A, “Analysis of Cybersecurity Standard and Framework Components,” Int. J. Commun. Netw. Inf. Secur, 12, 417–432, 2020.

[7] Collier, Z.; DiMase, D.; Walters, S.; Tehranipoor, M.; Lambert, J. Cybersecurity Standards: Managing Risk and Creating Resilience. Computer, 47, 70–76, 2014.

p-ISSN 2715-2871
e-ISSN 2714-5247

[8] ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection — Information security controls
[9] Eling, M. & Jung, K, "Heterogeneity in cyber loss severity and its impact on cyber risk measurement," Risk Management, 24(4), 273–297, 2022.
[10] Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A. & Stulz, R. M., "Risk management, firm reputation, and the impact of successful cyberattacks on target firms," Journal of Financial Economics, 139(3), 719–749, 2020.