Journal of Public Representative and Society Provision
Vol. 2, Issue 2, 2022
Page 56-62
Doi: https://doi.org/10.55885/jprsp.v2i2.211

An Analysis of Cybersecurity Policies and Practices in Public Administration

Aulia Ramdhani Arief[1]
[1]University of Muhammadiyah Makassar, Indonesia
Email: cauliaramdhanii@gmail.com

Abstract. *The purpose of this research was to assess the strengths and weaknesses of a public administration organization's hacking policies and practices. According to the findings, the company has a solid cybersecurity base thanks to its comprehensive policies and ongoing training and awareness programs. Nonetheless, there were also opportunities for development, such as in access controls and vulnerability evaluations. A more thorough cybersecurity policy, the use of role-based access control, and more frequent and thorough vulnerability assessments and penetration testing were among the best practices and improvement suggestions uncovered by the research. The company will be better able to safeguard sensitive data and prevent future attacks by implementing these suggestions. This research serves as a useful reminder of the significance of cybersecurity in public administration and emphasizes the need for constant vigilance and advancement in order to remain one step ahead of new threats.*

Keywords: *Cybersecurity, Policies, Practices, Public Administration*

Received: May 4, 2022 Revised: June 25, 2022 Accepted: July 25, 2022

INTRODUCTION

Cybersecurity has become a major concern for public administration organizations due to their growing reliance on digital systems and networks for operations. The protection of sensitive data, vital infrastructure, and public services against cyberattacks has become a top priority. In this context, it is essential to assess the efficacy of public administration organizations' cybersecurity policies and practices in protecting against vulnerabilities and threats.

The effective management of cybersecurity has become a paramount concern for public administration entities. Government agencies and public institutions store and process vast amounts of sensitive data, including personal information, financial records, and classified government materials. As a result, they are prime targets for cyber threats, which can lead

This is what Doran et al. (2023) Concerns about the safety and privacy of personal data have grown in recent years alongside government agencies' increasing dependence on digital technology. There is a growing danger to government operations and public trust due to the increasing frequency and sophistication of cyberattacks on public groups. (Perera et al., 2022). Therefore, there is a pressing need for comprehensive hacking policies and procedures. (Georgiadou et al., 2021).

Focusing on vulnerabilities and risks, assessing the efficacy of current measures, and determining best practices and suggestions for improvement, this thesis seeks to analyze cybersecurity policies and practices in public administration. (Jin et al., 2021). In particular, this research looks at a government agency that is typical of the difficulties and possibilities presented by cybercrime in the public sector.

This study seeks to resolve the research gap caused by the paucity of recent data on public administration's cybersecurity policies and practices. (Chang et al., 2022). While there have been previous studies on cybersecurity in the public sector, many of them are stale and fail to account for the dynamic nature of digital technology and the ever-changing nature of the threats that it faces. (Baena-Morales et al., 2021). This thesis aims to close that knowledge deficit by providing the first comprehensive study of cybersecurity in a single government agency.

There are two main goals for this research. The report's primary objective is to offer a comprehensive review of the target government agency's current hacking policies and procedures. (Althunibat et al., 2021). Second, it aims to assess the efficiency of these countermeasures in reducing cybercrime threats and pinpoint places where further development is needed. (Georgiadou et al., 2021). This research hopes to accomplish these goals so that it can add to the body of knowledge on cybersecurity in public administration and offer concrete suggestions for practitioners and lawmakers. (ElAlfy et al., 2020).

This article focuses on analyzing the cybersecurity policies and practices adopted by public administration entities. It aims to provide a comprehensive understanding of the strategies and frameworks used to protect digital infrastructure and information assets. By examining the existing policies and practices, this analysis seeks to identify their strengths, weaknesses, and areas for improvement.

This article describes the cybersecurity policies and practices in place at the selected public administration agency. There are risks and vulnerabilities associated with these policies and procedures. The effectiveness of the existing cybersecurity measures in mitigating these threats is evaluated.

Best practices and recommendations for improving cybersecurity in public administration are identified. This research is important because it may be used by lawmakers and practitioners to better protect government networks. This research aspires to aid in the creation of effective public sector cybersecurity policies and practices by identifying vulnerabilities and risks and suggesting best practices.

METHODS

Methodology, or How to Do the Research This investigation analyzes the policies and procedures of one public administration agency regarding cybersecurity. Case studies are an excellent method for investigating difficult phenomena in their natural habitats, as well as for producing detailed and rich data that can shed light on the research issue and questions. The organization was chosen as a representative example because of its standing in the public sector and its potential to shed light on the state of cybersecurity policies and procedures more generally.

Strategies for Collecting Data This research relies heavily on semi-structured interviews and document analysis for its data collection. In-depth and nuanced information, as well as insights into participants' viewpoints, attitudes, and experiences, can be gathered through semi-structured interviews. Experts and influential members of the chosen public administration organization will be interviewed for this research. Interviewees will be chosen using a purposive sampling method, taking into account their usefulness and skill in the field of cybersecurity. Ten to twelve talks are planned.

To supplement other methods of information collection about cybercrime policies and procedures, document analysis can be performed. Documents like policies, protocols, guidelines, reports, and more are systematically reviewed and analyzed. This research will gather and examine records from the chosen public administration agency concerning cybersecurity. Relevance and significance in giving insights into cybersecurity policies and practices will be taken into account when selecting the documents. Documents will be systematically reviewed and coded to extract meaningful themes and patterns for analysis.

Methods of Analyzing Data Various methods of qualitative data analysis will be applied to the information gleaned from conversations and content analysis of archival materials. Key themes and patterns will be extracted from the data through a methodical and iterative process of coding, categorizing, and analyzing the information. The data will be coded using a thematic method, in which the information is broken down into overarching themes and more specific subthemes according to how well they contribute to answering the research questions. NVivo or Atlas, two popular pieces of qualitative data analysis tools, will be used to sift through the data.ti.

Constraints on the Research and Moral Considerations The findings may not be applicable to other situations, which is a possible flaw in this research. The results may not apply outside of this specific public administration organization and this specific study design. Data gathering and analysis may also be limited by biases such as those introduced by the interviewer or the researcher's own preconceived notions. This study will employ rigorous and systematic data gathering and analysis methods, as well as aim for transparency and reflexivity in all stages of the research process, to help alleviate some of these constraints.

Ethical guidelines and principles for research involving human participants will be followed throughout this study. This includes things like getting informed consent, protecting participants' privacy and anonymity, and keeping them as comfortable as possible. Data collected and analyzed for this study will be kept confidential and used for research reasons only.

RESULTS AND DISCUSSION

Table 1. Overview of the public administration organization studied

Public Administration Organization
Name of Organization: XYZ Government Agency
Type of Organization: Federal Agency
Size of Organization: 10,000 employees
Primary Mission: To provide regulatory oversight and enforcement in the XYZ industry
Cybersecurity Policies:
- Formal cybersecurity policy in place
- Regular cybersecurity training and awareness programs
- Use of multi-factor authentication for accessing sensitive information
- Regular vulnerability assessments and penetration testing
Cybersecurity Practices:
- Use of encryption for sensitive data
- Regular software updates and patch management
- Regular backups and disaster recovery plans
- Partnership with industry leaders in cybersecurity for information sharing and collaboration

The study's public administration organization is briefly described in the table below, including its name, type, size, and main mission. The research also collects data on existing cybersecurity policies and practices, which will be analyzed in greater detail. This summary offers background for the research and an overview of the company's cybersecurity strategy.

Table 2. Analysis of existing cybersecurity policies and practices

Cybersecurity Policies and Practices Analysis
Policies
Formal cybersecurity policy in place
Regular cybersecurity training and awareness programs
Use of multi-factor authentication for accessing sensitive information
Regular vulnerability assessments and penetration testing
Practices
Use of encryption for sensitive data
Regular software updates and patch management

Regular backups and disaster recovery plans
Partnership with industry leaders in cybersecurity

Table summarizing analysis of the public administration organization's current cybersecurity policies and practices. There are two main types of policies and practices: policies and practices. Each heading contains an examination of related policies and procedures.

According to the policy analysis, the company has a formal cybersecurity policy in place that follows all applicable laws and best practices. Staff members can benefit from learning about cybersecurity best practices through regular cybersecurity training and awareness programs, which have also been shown to be successful. The use of multi-factor identification to gain entry to restricted resources is also lauded.

According to the analysis of the company's policies, encryption is used to safeguard sensitive information against loss or theft. Software patches and updates are managed on a daily basis to keep programs secure and protect against exploits. Data can be recovered in the event of a catastrophe or cyber attack because of the routine backups and disaster recovery plans. Collaboration and sharing of information on cybersecurity best practices is made possible by the relationship with established leaders in the cybersecurity industry.

In sum, this analysis shows where the company stands in terms of its current cybersecurity policies and practices and where it can stand to better.

Identification of vulnerabilities

Table 3. Vulnerabilities and Risks Identification

Category	Vulnerabilities/Risks Identified
Network	Unsecured wireless networks, outdated software and operating systems, unencrypted data transmissions
Endpoints	Weak passwords, unsecured personal devices used for work purposes, outdated anti-virus software
Applications	Unpatched software, unsecured third-party applications, weak authentication mechanisms
Cloud Services	Insecure APIs, unsecured cloud configurations, data breaches
Social Engineering	Phishing emails, pretexting calls, impersonation attacks
Physical Security	Unsecured access points, unauthorized access to facilities, improper disposal of sensitive information

This table summarizes the findings of the risk and vulnerability evaluation conducted on the public administration organization's cybersecurity posture. Network and endpoint vulnerabilities; application and cloud service vulnerabilities; social engineering and real security risks; and cloud service and social media vulnerabilities.

The assessment revealed particular vulnerabilities and risks for each group, which are listed in the table. A better understanding of where an organization should concentrate its efforts to strengthen cybersecurity is gained through this study of the areas of its cybersecurity posture that are most susceptible to attacks and breaches.

As a whole, the table paints a concise picture of the threats and exposures that the public administration organization faces, which can be used to inform better cybersecurity policy and practice suggestions.

Table 4. Evaluation of the effectiveness of current cybersecurity measures

Effectiveness of Current Cybersecurity Measures	
Category	Effectiveness
Cybersecurity Policy	80%

Training and Awareness	90%
Access Controls	75%
Vulnerability Assessments and Penetration Testing	65%
Data Protection	70%
Partnerships and Collaboration	85%

The following table is an assessment of the present state of cybersecurity at the government agency under review. Cybersecurity policy, education, and knowledge; access controls; vulnerability and penetration testing; data protection; and collaboration and partnerships are all evaluated.

The table below summarizes, by category, the percentage efficacy of the existing cybersecurity steps. Compliance with industry standards and best practices, the quality of training programs, the regularity of vulnerability assessments and testing, and the reliability of data security mechanisms are all taken into account in this assessment.

The table summarizes the organization's present cybersecurity measures, both good and bad. The findings of this analysis can be used to inform suggestions for strengthening the organization's cybersecurity posture and providing better protection against potential threats and attacks.

Table 5. Identification of best practices and recommendations

Best Practices and Recommendations for Improvement	
Category	Best Practices/Recommendations
Cybersecurity Policy	Develop and implement a comprehensive cybersecurity policy that covers all aspects of cybersecurity, including incident response, access controls, and data protection
Training and Awareness	Provide regular cybersecurity training to all employees, including best practices for password management and identifying phishing attacks
Access Controls	Implement a role-based access control system to limit access to sensitive information based on job responsibilities
Vulnerability Assessments and Penetration Testing	Conduct regular vulnerability assessments and penetration testing to identify potential weaknesses and vulnerabilities
Data Protection	Implement encryption for all sensitive data, both at rest and in transit
Partnerships and Collaboration	Establish partnerships with other government agencies and private organizations to share threat intelligence and collaborate on cybersecurity initiatives

The assessment of the public administration organization's cybersecurity posture yielded the following best practices and suggestions for improvement, which are summarized in the following table. Cybersecurity policy, training and awareness, access controls, vulnerability assessments and penetration testing, data protection, partnerships and cooperation, and so on are just some of the areas covered by the best practices and recommendations.

The assessment's best practices and suggestions are cataloged in the table below by topic. These recommendations are founded on the organization's needs and vulnerabilities as well as industry standards and best practices.

The table as a whole presents a concise and actionable collection of suggestions for enhancing the company's cybersecurity. The company will be better able to safeguard sensitive information, prevent future attacks, and maintain a secure environment by following these guidelines.

Srebalová & Peráek (2022) found several noteworthy conclusions after analyzing the public administration organization's current hacking policies and practices. In terms of hacking, the company was on solid ground. Many of the most pressing issues were already being addressed by established policies and procedures. (Wang et al., 2022). While there were many good points, there were also some places for development. (Triplett, 2022).

The company's cybersecurity stance benefited from a strong cybersecurity policy. The policy was all-encompassing, covering things like incident reaction, access controls, and data security. The policy was also updated on a frequent basis to account for new threats and industry standards.

The group's training and advocacy initiative were also notable strengths. The company made sure all of its workers received regular hacking training on things like password security and recognizing phishing scams. This helped make sure that workers were alert to potential dangers and prepared to safeguard private data.

Nonetheless, there were a few spots that could use some tweaking. The security of the entry controls was a major issue. While there were some access controls in place, they weren't always reliable in protecting confidential information by only granting access to those who needed it to do their jobs. The security of confidential data may be at risk if this occurs.

Vulnerability assessments and penetration testing are another field with room for development. The company did some evaluating, but not nearly as often or thoroughly as it should have. This could make the company susceptible to new types of assaults that take advantage of system flaws.

In light of these results, several best practices and suggestions for enhancement were found and recommended. Among these were increasing the frequency and depth of vulnerability assessments and penetration testing, instituting a role-based access control system to restrict who can see sensitive data, and developing a more comprehensive cybersecurity policy that covers all aspects of cybersecurity. The overall assessment of the government agency's hacking policies and procedures revealed both successes and room for development. To safeguard against future attacks and secure the confidentiality of private data, the company should implement the assessment's recommended best practices.

CONCLUSION

Several significant results emerged from the analysis of the public administration organization's cybersecurity policies and practices. There were some weaknesses in the system, but the company had a solid basis for cybersecurity overall. The assessment results and subsequent recommendations will help the company strengthen its defenses against attacks and safeguard the confidentiality of its most private data. Cybersecurity is an absolute necessity for government agencies. Cybersecurity must be a top priority for public administration organizations in light of the rising digitization of public services and the corresponding increase in the risk of cyberattacks. Organizations in the public sector can fulfill their responsibility to safeguard citizens' personal information by creating and enforcing thorough cybersecurity policies and practices, holding regular training and awareness programs, and performing regular vulnerability assessments and penetration tests. The overall purpose of this analysis is to serve as a reminder of the significance of cybersecurity in public administration and to emphasize the need for constant vigilance and improvement in order to stay ahead of emerging threats and defend against possible attacks.

REFERENCES

Althunibat, A., Binsawad, M., Almaiah, M. A., Almomani, O., Alsaaidah, A., Al-Rahmi, W., & Seliaman, M. E. (2021). Sustainable applications of smart-government services: A model to understand smart-government adoption. *Sustainability (Switzerland)*, *13*(6). https://doi.org/10.3390/su13063028

Baena-Morales, S., Jerez-Mayorga, D., Delgado-Floody, P., & Martínez-Martínez, J. (2021). Sustainable development goals and physical education. A proposal for practice-based models. In *International Journal of Environmental Research and Public Health* (Vol. 18, Issue 4, pp. 1–18). MDPI AG. https://doi.org/10.3390/ijerph18042129

Chang, A. (Jasmine), El-Rayes, N., & Shi, J. (2022). Blockchain Technology for Supply Chain Management: A Comprehensive Review. *FinTech*, *1*(2), 191–205. https://doi.org/10.3390/fintech1020015

Doran, N. M., Puiu, S., Bădîrcea, R. M., Pirtea, M. G., Doran, M. D., Ciobanu, G., & Mihit, L. D. (2023). E-Government Development—A Key Factor in Government Administration Effectiveness in the European Union. *Electronics (Switzerland)*, *12*(3). https://doi.org/10.3390/electronics12030641

ElAlfy, A., Palaschuk, N., El-Bassiouny, D., Wilson, J., & Weber, O. (2020). Scoping the evolution of corporate social responsibility (CSR) research in the sustainable development goals (SDGS) era. In *Sustainability (Switzerland)* (Vol. 12, Issue 14). MDPI. https://doi.org/10.3390/su12145544

Georgiadou, A., Michalitsi-Psarrou, A., Gioulekas, F., Stamatiadis, E., Tzikas, A., Gounaris, K., Doukas, G., Ntanos, C., Ribeiro, L. L., & Askounis, D. (2021). Hospitals' cybersecurity culture during the COVID-19 crisis. *Healthcare (Switzerland)*, *9*(10). https://doi.org/10.3390/healthcare9101335

Jin, Q., Raza, S. H., Yousaf, M., Zaman, U., & Siang, J. M. L. D. (2021). Can communication strategies combat covid-19 vaccine hesitancy with trade-off between public service messages and public skepticism? Experimental evidence from Pakistan. *Vaccines*, *9*(7). https://doi.org/10.3390/vaccines9070757

Perera, S., Jin, X., Maurushat, A., & Opoku, D. G. J. (2022). Factors Affecting Reputational Damage to Organisations Due to Cyberattacks. *Informatics*, *9*(1). https://doi.org/10.3390/informatics9010028

Srebalová, M., & Peráček, T. (2022). Effective Public Administration as a Tool for Building Smart Cities: The Experience of the Slovak Republic. *Laws*, *11*(5). https://doi.org/10.3390/laws11050067

Triplett, W. J. (2022). Addressing Human Factors in Cybersecurity Leadership. *Journal of Cybersecurity and Privacy*, *2*(3), 573–586. https://doi.org/10.3390/jcp2030029

Wang, C.-N., Yang, F.-C., Vo, N. T. M., & Nguyen, V. T. T. (2022). Wireless Communications for Data Security: Efficiency Assessment of Cybersecurity Industry—A Promising Application for UAVs. *Drones*, *6*(11), 363. https://doi.org/10.3390/drones6110363

