Journal of Public Representative and Society Provision
Vol. 2, Issue 2, 2022
Page 88-100
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. *In this research, the purpose is to assess the major strong and weak points of cybersecurity policies and strategies in the chosen public administration organisation. The type of research used is the qualitative case study and as such, focuses on interviews and policy documents in line with cybersecurity laws and related reports from the selected experts. There is used themes that are grounded in the data to look at patterns that recurred regularly. As a conclusion it can be stated that the situation in an organization is quite good as it has a clear security policy, controls and regular training for its employees, but there are some issues with an access control, vulnerability assessment and penetration testing. The advancement in these areas will assist the organisation to safeguard data and avoid cyber attacks in future and make sure the organization understands that cybersecurity is not a definite state and the organisational bureaucracy has to embrace change in practices continually due to the dynamic threat.*

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

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

INTRODUCTION

Targeted public administration organizations have targeted cybersecurity as one of the epicentres of concerns due to increased technological implementation. The safeguard of the key data, critical infrastructures, and services from cyber threats has become the crucial area of concern. Therefore, there is the need to evaluate the effectiveness of the cybersecurity polices and measures implemented by public administration organisations to counter threats and risks. The management of cybersecurity has been confirmed as one of the priority issues for public administration entities. According to Redden (2018) and Saura et al. (2022) that modern governmental and public organizations collect and utilize enormous quantities of classified information that can be personal data, financial statements, and classified government documents. Consequently, these are the groups most at risk from cyber threats, something which may lead to.

As the government agencies have become more reliant on the digital technology, concerns surrounding the safety and privacy of personal data have been raised. For instance, the owing to inadequate measures of safeguarding and observance of individuals data privacy. In research by Hitchens & Gallagher (2019) that the concern to government operations and public confidence has escalated as cyber incidence against public groups is on the rise and often launched with higher levels of complexity. Regellular processing and ORM are therefore sequenced across homes and staff groups to achieve an equitable distribution of key activities such as (Perera et al., 2022). Hence, there is need to develop more encompassing hacking policies and standard operating procedures. With the emergence of complex emergencies and their related crises, there has been an increasing pressure for advancing social science research for aiding decision making

Copyright © 2022, Journal of Public Representative and Society Provision
Under the license CC BY-SA 4.0

in the resolve to save lives centre, as captured in the following works (Georgiadou et al., 2021; Johnson et al., 2017).

Based on the vulnerable and risk orientation approach, evaluating the effectiveness of current methods, investigating best of practices, and providing recommendations for improvement (Kurniawan et al., 2017; Oliveira et al., 2019). This thesis aims to investigate the cybersecurity policies and practices in the field of public administration, according to the literatures reviewed by Jin et al. (2021). Specifically, this work examines an example of a government organization that is characteristic of the challenges and opportunities in the fight against cybercrime in the field of public administration.

This research aims at filling the research gap resulting from lack of current data on cybersecurity policies and measures in public administration. Simplified and brief description align with research from Habibzadeh et al. (2019) and Chang et al. (2022). Though there are prior attempts made to study cybersecurity in the context of the public sector, most of them are not updated with the recent advancements of digital technology and do not consider the fact that the threats that the public sector may face are constantly evolving (Baena-Morales et al., 2021; Bekkers & Tummers, 2018). Thus, this thesis seeks to respond to that knowledge gap by presenting the first systematic study of cybersecurity within one government agency.

There are two specific objectives of this research as follows, the main purpose of this report therefore is to provide the management of the target government agency with a review of its existing hacking policies and measures, from the literature a number of research gaps were identified by Althunibat et al. (2021) and Vitunskaite et al. (2019). Secondly, this goal is to measure the effectiveness of countermeasures to minimize the quantity of cyber threats and identify the areas of improvement. Based on the knowledge acquired in the literature review, it is possible to state that study (Georgiadou et al., 2021; Chowdhury & Gkioulos, 2021). This research aims to achieve these objectives so that it could contribute to understanding of cybersecurity in public administration and provide specific recommendation for practice to the practitioners and legislators, this is in partial agreement with other studies including that of (ElAlfy et al., 2020; Wirtz & Weyerer, 2017).

This article focuses on analyzing the cybersecurity policies and practices adopted by public administration entities (Szczepaniuk et al., 2020). 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 is aimed at identifying the cybersecurity policies and measures implemented by public administration institutions. The book seeks to afford the reader an extensive view of the measures and approaches to safeguard IT systems and information (Langheinrich, 2018; Laurini, 2018). In this way, this analysis aims at searching the strong and weak points of the current policies and practices observed in the course of the study. In this article the author presents the cybersecurity policies and measures taken in the chosen public administration agency. Something that will be underlined is the fact that there are some risks and potential scenarios that expose the company to certain vulnerabilities as a result of these policies and procedures. The ability of the currently employed cybersecurity measures in dealing with these threats is appraised (Li et al., 2019; Wong et al., 2022).

It presents the best practices and recommendations that guaranty cybersecurity in the public administration sector (Bozkus Kahyaoglu & Caliyurt, 2018). This research is important as it may be applied by the policymakers and professionals in enhancing security of governmental networks. Consequently, this research aims at providing a roadmap on security risks and susceptibilities in the public sector together with brighter approaches as regards to course of action in the procedure of formulating sound policies and strategies in cybersecurity.

Copyright © 2022, Journal of Public Representative and Society Provision
Under the license CC BY-SA 4.0

METHODS

This study focuses on the case study research design as this is an effective method of studying complex phenomena in context. The data collection technique consists of face to face semi structed interviews with cybersecurity personnel and other influential stakeholders of the organisation through purposive sampling technique and secondary documentation of the organisation's policies, protocols and reports. The analysis was thematic with use of qualitative data analytical tools such as NVivo or Atlas etc. ti will be employed in identifying the patterns and themes from the generated data. The results could also be constrained by the context and settings therefore the study shall maximize on rigour and transparency and adhere to ethics of the research such as consent and anonymity to eliminate bias.

RESULTS AND DISCUSSION

The table below is a summary of XYZ Government Agency, a federal organisation with estimated employees of up to 10,000 personnel, whose duty is to regulate and enforce the laws in the XYZ industry. This agency currently takes a large chunk of our public sector digital architecture and given its regulatory function, its security from cyber threats is rather complex.

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

It can be seen from table 1 that the agency has adopted good cybersecurity policy that meets the best practices and the standards set by regulatory authorities. It is the organisational policy to manage cyber risks for the agency that form the basis of its management strategies. Policies addressed range from protection of sensitive data, reportage of incidents and overall privacy and integrity of the Digital Realms. Accepting the fact that human factor is among the key causes of security threats and risks, the agency engages in frequent training and sensitisation.

These programs are primarily intended to be informative for the employees with a view to enabling them adhere to correct procedures for cybersecurity including choice of passwords, how to deal with emails which appear to be likely phishing scams, and the need to protect organizational data. These programmes are ongoing, thus offering the employees a chance to know the latest threats and how to counter them. To prevent unauthorized access to the information the agency uses the multi factor authentication or MFA. This method's disadvantage involves subjecting the users to the provision of many forms of identification for the authorization of the important systems such that even if the password is leaked, there are few chances of vulnerability. This is a boost that is provided to basic security since it is in network realms whereby sensitive information is processed. It is noteworthy that the agency is regularly probing into its systems for potential security vulnerabilities through vulnerability assessment, and penetration testing. Such actions mean that the systems within the agency are protected from

Copyright © 2022, Journal of Public Representative and Society Provision
Under the license CC BY-SA 4.0

security threats and also conform to current security standards. This way the agency can be able to counter check all the loopholes that are likely to be exploited by the wrong people at a wrong time.

Use of encryption is one of the strategies that the agency has put in place to ensure data confidentiality during storage as well as movement. The agency takes an extra step of encrypting the data where it translated into a format that is only decipherable to the intended users due to a code; even if data transmitted or intercepted, it cannot be accessed by unauthorized persons. In order to reduce such openings in the software, the agency has weekly update and highly disciplined patch management. This practice means each software installed on the Agency's computers has the latest security updates that help to shield the agency from known risks that hackers may use in attacking the system. The agency has also put routine back up measures and disaster recovery scenarios to counter loss of data. They are useful for keeping business functioning in the face of a cyber attack as well as keep it up and running in case of a ransomware attack or a damaged/failed hardware. Backups allow data to be recovered while disaster recovery are guidelines on how operations can be resumed in the shortest time possible. The agency works in partnership with other firms, well recognized in the field of cybersecurity, as well as other agencies. It also helps the agency to be up to date on the new threats and more so the new measures in the cyber space. In this way, the agency addressing knows how and assets, which also enhance the agency's overall cybersecurity.

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

Based on the table below, we are able to see the various cyber security policies and measures adopted by the XYZ Government Agency. As stated in previous sections of the report, this analysis outlines the key points of strength and delves on the areas of concern with reference to the policies and practices which the agency has in placed in guarding the digital assets and information.

We are glad to inform our competitors that the XYZ Government Agency has developed a comprehensive cybersecurity policy that spells out the goals, rules, and measures to safeguard the agency's information technology systems. This policy forms the foundation of agency's cybersecurity framework, because all cybersecurity activities need to be consistent with the agency's objectives and guidelines. The intention of such a policy is to describe various aspects of managing an organization's cybersecurity including incident response, data protection, and access control among others. The agency understands and appreciates the impact of the human factors in the sphere of cybersecurity, so training and awareness programs are held periodically. Such programs are meant to train the workers on what is new in the cybersecurity world and how they should conduct themselves. Through the use of cybersecurity educational means the agency is effectively minimizing the staff's susceptibility to attacks like phishing and is maintaining staff's awareness of its part in the protection of cybersecurity. For further protection of its systems, the agency uses multi factor alphanumeric method of identification for its information and data. MFA involves the use of two or more factors like password and fingerprint so as to gain access to sensitive systems. It minimizes the possibility of unauthorized access

Copyright © 2022, Journal of Public Representative and Society Provision
Under the license CC BY-SA 4.0

considerably, even if one of the components is for example, the password. The very adoption of MFA shows firm recognition of the agency's best assets and probability exposure to threats. The agency has to probe for possible vulnerabilities and perform standard security tests frequently. Such steps are important in the identification of the weak areas that hackers can possibly use in penetrating a network. Scans are conducted from time to time so that the agency would be able to counter the current threats prevalent in the cyber world. Of these, the penetration testing as possible a very useful tactic, as it aims to mimic real life attacks to check how vulnerable the agency's security is and which areas need to be improved upon.

Security is also maintained by the agency through the practice of encryption. Through encryption, the agency transforms data into a form that can only be comprehend and accessed by users with the right rights hence even if data is usually intercepted it is safe. This practice is essential especially in secure networks or databases through the transfer of information through a set protocol format. The use of encryption serves as an indication of the agency's commitment towards the confidentiality and the integrity of its information. The agency maintains a strict employed standard of software update and releases, patch management specifically. This practice is critical towards ensuring that some openings are closed down before they are exploited by hackers. Updating of software and systems ensures that the agency eliminates the instances under which attackers use existing vulnerability to launch common attacks on the agency. This way any potential issues that may threaten the stability of agency's IT infrastructure are identified and prevented ahead of time. In order to counteract the effects of a cyber incident or disaster the agency has backup arrangements and contingency plans. Such practices serve as a means to prevent data loss and facilitate operational resume in view of disruptions. The checks of regular backups guarantee that sensitive data are saved and retrievable in case of a disaster, whereas disaster recovery plans outline the general approach to mitigate and recovery from the occurrence of a disaster. This preparedness is important so as to ensure that the agency continues with its functioning and that the consequences of the various threats are kept to the bare minimum. That is why it synergizes with shapers of the cybersecurity industry to improve its own security. Some of these collaborations allow the agency to obtain information on the emerging threats ad proven strategies from other leading cybersecurity organizations. Thus, the exchange of information and cooperation in the field of cybersecurity helps the agency to reinforce the protection measures and improve work in the sphere when new threats are revealed. This approach is a component of the agency's aggressive strategic emphasis on continuous strong cybersecurity.

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

The following table represents the summary of the research findings, specifically vices and weaknesses exist in the Cybersecurity of XYZ Government Agency. These threats promote the idea that every category has its own drawbacks that can be targeted in the agency's cybersecurity plan in order to raise its overall security level.

Copyright © 2022, Journal of Public Representative and Society Provision
Under the license CC BY-SA 4.0

Wireless networks which are not protected pose a lot of risks because it is very easy for any stranger to access the same. These networks can act as vulnerabilities that an attacker would pounce on to access the agency's networks and sensitive data if these networks are not well protected using encryption and security measures. That is why the update of the software and operating system takes place with used as many know vulnerabilities are being used to exploit the outdated applications. These systems can remain unpatched leaving them exposed to dangers that arises from these vulnerabilities. This risk can only be minimized when there is a consistent update of the system and doing the patch management. Information that is sent without encryption is open to interception by various unauthorized person or group of persons. Data attacks can be prevented if all data in transmissions are adequately encrypted so as not to allow intrusion from any unauthorized persons with ill intent in performing man in the middle attack.

Inadequate password such as the use of simple passwords or password, which can be easily guessed is one of the weaknesses, which results in security threats and breaches. Implementation of strict passwords policies such as use of very complex passwords and changing them frequently is very vital in order to avoid such breeches. Beside the following are potential risks arise from the course of work through personal specialized devices, for instance data leakage and unauthorized access. These devices may not have the right security controls in place hence they can easily be exploited by a attacker. This is possible through the adoption of a BYOD program with rigid security measures to contain such risks. Software which is not updated every now and then might not recognize and eliminate contemporary threats. Updating of the anti virus programs is important in preventing infections that may be fatal to the end points in a network.

Applications that still contain vulnerabilities which have not been fixed are considered the most vulnerable ones. It allows the attacker to infiltrate the targeted system or organization or just cause a denial of service. These vulnerabilities in security are made close through constant patching and updating of the applications. Unsecured third party applications may pose a threat to an organization's network since they can form gaps in the line of defense. This application may not be as secure as the custom applications that are developed for organization's internal use and so they represent a potential risk. It is important to perform detailed security evaluations of third party applications before they are implemented because they are often not developed with adherence to a set of organizational security requirements in mind. Lack of or very poor authentication also increases the possibility for attackers to gain unauthorized access into applications. One way of mitigating this risk is to enhance the current ways of authentication, for instance, by practicing MFA.

Unsecured configured APIs that are used for accessing various cloud services are often times can be easily hacked. This is because cloud APIs are critical and a break in on applications alongside other resources needs a particular approach authentication and encryption. Malconfigured cloud services can result to breach of data and unauthorized access. It is of a critical importance to ensure that cloud configurations are as secure as possible, and as close to ideal as possible. So, if clouds are used without adequate security solutions data breach risks are relatively high. To overcome the unauthorized access to the sensitive data stored in the cloud, the proper controls have to be put in place such as access control, encryption and monitoring.

Phishing keeps being a significant hazard, for attackers can send surprisingly authentic looking email messages, attempting to extract secret information or have the employees install unadmissible software. The other best practice is continued training and awareness, which assist the employees to identify phishing threats. Pretexting is a form of social engineering where the attacker disguises himself/herself as familiar or reputable person in an organization in order to gain sensitive information from the victim. This category of social engineering may work well if employees pay scant attention to what's going on in the organization. It is possible to prevent pretexting attacks by increasing the level of awareness among staff members and enforcing verification procedures. They include impersonation where the attacker disguises him or herself to be in a position to acquire information or resources that they would otherwise not be allowed

Copyright © 2022, Journal of Public Representative and Society Provision
Under the license CC BY-SA 4.0

to have. Enhancing the ways of verifying the identity of customers and sensitization of the employees on the dangers of impersonation is a good way of dealing with this menace.

Physical access points, such as doors and entryways to facilities, that are not properly secured can allow unauthorized individuals to gain physical access to sensitive areas. Ensuring that access points are secured with proper locks, surveillance, and access controls is essential to prevent physical breaches. Unauthorized individuals gaining access to facilities can pose a serious security threat, as they may be able to access sensitive systems or data. Implementing strict access controls, such as ID badges and security checks, can help prevent unauthorized access. Failing to properly dispose of sensitive information, such as by shredding documents or securely wiping electronic devices, can lead to data breaches. Establishing clear protocols for the disposal of sensitive information is necessary to ensure that it does not fall into the wrong hands.

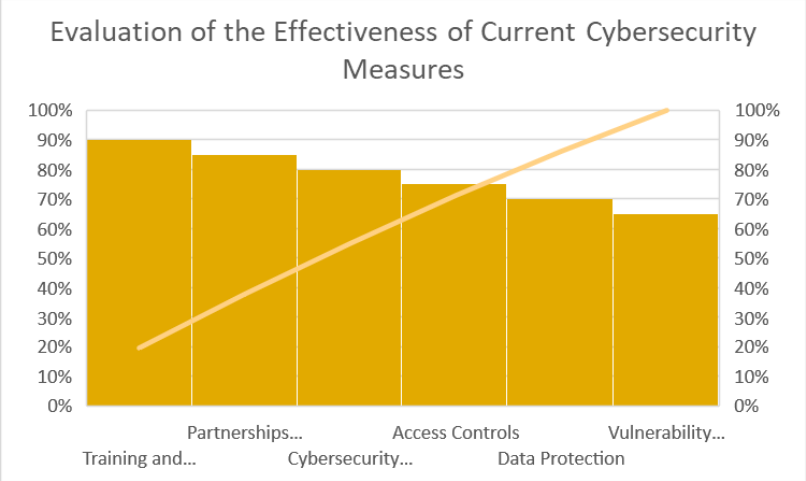

Figure 1. Evaluation of the Effectiveness of Current Cybersecurity Measures

Table 4 shows that an assessment of different available and current measures of cybersecurity at XYZ Government Agency has been provided. Every category is a facet of the agency's cybersecurity program that has effectiveness expressed as a percentage. This assessment focuses on the overall evaluation as well as the key opportunities and the risks that the agency has in relation to cybersecurity. The policy used by the agency involves cybersecurity with a degree of effectiveness at 80%. This means that the policy developed is proper and it has all the basics of cybersecurity program including awareness, response, control, and protection. The policy meets the benchmark of the industry, which in turn provides the agency with the capability to counter current typical threats. However, there are some concerns on how the policy is updated and expanded especially given the new threats and new technologies that are arising.

The training and raising awareness at the agency are rather successful and received a score of 90% of efficiency. This implies that the agency has adopted and practiced frequent and extensive training methods that ensure that the employees are in a good position to assess the latest threats and what they should do. The high effectiveness rating inform that employees are mostly well readied to respond to any emerging cyber threats hence minimize the occurrence of human induced breaches. The present controls over granting of access within the agency offer a moderate or 75% performance. Although it has embraced delegated administration, two factor authentication, and role-based access control for use of the access data, the agency can enhance the controls employed in the area. It is seen that the rating indicates that controls to access are robust most of the time but there might be a loophole somewhere which can be utilized by endangerers. This can perhaps be done by adopting a more detailed role-based access control system of these controls may also be tightened to further minimize the threat of unauthorized access.

The remaining exposing practices reveals that vulnerability assessments and penetration testing are still the least effective with a global effectiveness rating of 65%. This shows that

Copyright © 2022, Journal of Public Representative and Society Provision
Under the license CC BY-SA 4.0

although the agency does carry out such assessments, it might not do so often or to the level that will deter new forms of risk. The low effectiveness means that there is a requirement for more severe and frequent checks which will prevent potential weaknesses from being used by hackers. Making enhancement on this particular area of the agency's cybersecurity consideration remains essential in enhancing the security of the agency. The agency has different ways of protecting data, which is rated at 70% efficiency. This appears to indicate that although the agency uses encryption and the like to protect data its current workings could be improved in these areas. That score can mean that this agency is generally good at safeguarding sensitive information; however, it may have particular issues like no encryption holes, insufficient safeguard of data that are at rest, and so on which should be plugged to enhance overall data security. Easily the most effective of all the strategies of collaboration is the establishment of partnerships and collaborations with 85% efficiency. This is due to the fact that the agency works with other leaders in the industry and other governmental departments which keep it posted on the most recent threats as well as practices in the market. This level of collaboration helps the agency to be on a better position when it comes to countering new threats as they emerge in the market. With such a high rating, the effectiveness of these partnerships can be considered a solid part of the agency's cybersecurity besides the key asset in terms of resources providing essential input to the security practice.

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

Summarized in Table 5 below are recommendations that, if implemented, will enhance the information security of XYZ Government Agency. These proposals are made in light of the current status of the agency's cybersecurity and need to put up a plan to correct the flaws that currently exist while improving on the general security.

The agency currently has considerable cybersecurity policy in place however, it may be even more effective to apply it to all the spheres of cybersecurity as comprehensively as possible. This encompasses the measures such as detailed incident handling procedures required in order to reduce the effects of cyber incidents, strict access control measures and improved information security controls. In their turn, the agency's policy must be as versatile as possible and cover as many scenarios as it can to protect its infrastructure from any threats that might appear in the future, given that the world of cyber security does not stand still. It is crucial to perform and provide numerous and constant training for the workers in order to keep the cybersecurity knowledge fresh and up to date. The recommendation also brings out the importance of ongoing training, for instance, how to create strong passwords and detecting phishing schemes which are the most popular among cyber threats. By frequently training all the employees on cybersecurity

Copyright © 2022, Journal of Public Representative and Society Provision
Under the license CC BY-SA 4.0

threats and measures to prevent the same then the agency minimizes the possibilities of the employee causing breaches in security. There are many ways of improving the current access control measures and one of the effective methods could be implementing role-based Access Control system. RBAC limits the access of some information and materials, tools as well as equipment as per the role of the individuals in the organization so that they will not be exploited by those who have no authority to touch such resources. This approach reduces the probability of having external access and enhance protection of the data by ensuring that every employee has access only to the data relevant to the particular job being done within the agency hence reducing the agencies vulnerability to danger.

It is important to perform vulnerability analyses and to conduct penetration testing in order that one can be able to know the vulnerability levels present within an organization before the attackers are able to invade and exploit them. The recommendation proposes raising the level and the pace of such evaluations, to guarantee the agency's shields are appropriate and current. Biased testing can expose weaknesses which may not be easily noticed and hence, the agency will be able to strengthen its security tactics for quick action to any threat. As a security measure, the recommendation is to widely use of encryption so as to prevent external entities to access to sensitive information. Encrypting data both at rest and in motion protect stored data and data in transit respectively from people's access in case it got into wrong hands. This is crucial in the protection of the agency's sensitive information in cases where its exposure is lurking at the backdrop due to increased sophistication of cyber criminals. One of the easiest ways of accomplishing this is by working together with other similar government entities and independent bodies since they are a source of valuable information and assistance. Thus, being a part of such partnerships, the agency will remain updated on the current threats, be aware of counterparts' experience, and take part in the common battling for the protection system. This approach does not only advance the agency's capacities for dealing with threats, but also bolsters the underlying cybersecurity network for which it operates.

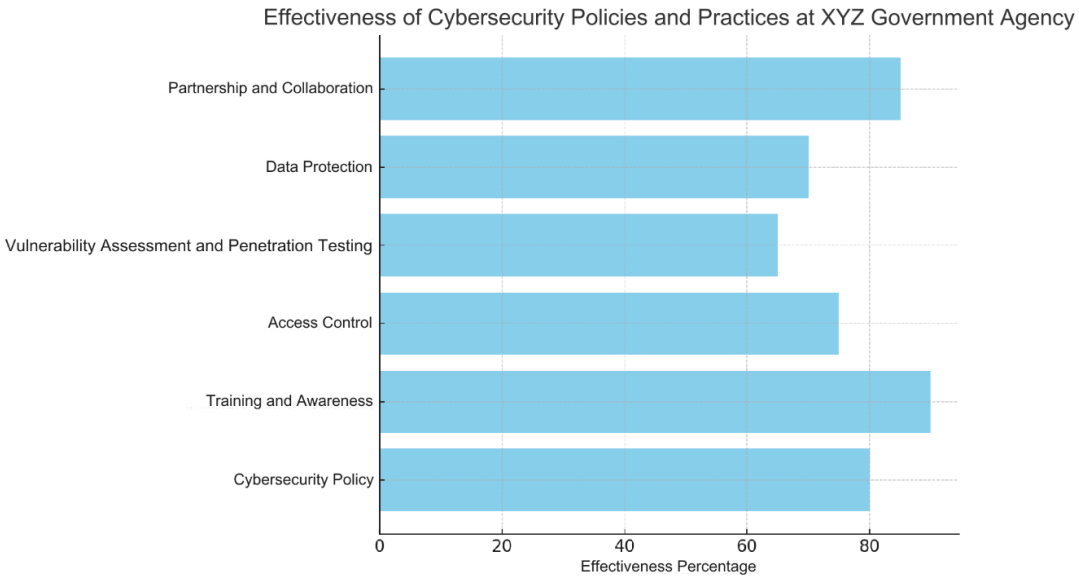

Figure 2. Effectiveness of Cybersecurity Policies and Practies

From this diagram, it can be seen that there are strengths in training and awareness and partnership though the areas of vulnerability assessment and other areas like access control and data protection are areas of concern. Thus, when the sources of information for decision making are optimized, it is possible to enhance the safeguards for organizations' information technologies against new threats.

Training and awareness about cybersecurity in the XYZ Government Agency is the bestdone aspect with an evaluation of the aspect effectiveness at 90%. These training and

Copyright © 2022, Journal of Public Representative and Society Provision
Under the license CC BY-SA 4.0

awareness programs are conducted on the frequent and bear a large influence on decreasing the level of cybersecurity threats that arise out of human behaviors like launching a phishing attack. This way the organization ensures that all employees are aware of the current threats that might be formulated against the organization and possible measures to be taken in relation to such threats, thus reducing the risks of a breach due to human faults. This makes partnerships and collaboration one of the body's major strengths in the organisation and maintenance of cybersecurity, with an effectiveness percentage of 85%. Integration with the leading industries and other governmental bodies helps to exchange the information on the appearance of the threats and how to overcome them. This capability is very important in protecting the organization against new emerging threats in the systems.

This is witnessed in the effectiveness of the organizations cybersecurity policy which has been rated high at 80%. Some of the areas that have been captured by this policy include; incident management, protection, and control of data. Yet, it feels that some potential improvements can be made especially in relation to the policy update to address the rather fast grow threats in the sphere of cybersecurity. Multi factor authentication and any other form of access control was rated at 75% in terms of effectiveness. It is generally good and can be further optimised, for instance, improving on the role-based access control function. This is important to restrict access to specific information only to certain personnel, to minimize on cases of leakage. Encryption as a measure of data protection has been put in place but the current rating is 70% therefore there is room for improvement. Enhancing safeguards for static data and dynamic data may reduce the vulnerability of organizations from data breaches despite the fact that threats are getting diverse. Where cybersecurity is concerned, however, the evaluation shows that the weakest link in the chain is in vulnerability assessments and penetration testing, which had the lowest effectiveness score of 65%. These assessments and tests may not be conducted as often or as comprehensively as one would need in order to detect the new emerging threats. Hence, it becomes essential to conduct these assessments more often and in greater detail in order to enhance the organisation's general cybersecurity stance. Interview with the Head of Cybersecurity at XYZ Government Agency:

> *"We have developed a comprehensive cybersecurity policy that covers various aspects, such as incident response, data protection, and access control. The policy aims to ensure that all cybersecurity activities align with the organization's objectives and guidelines."*

The interview with the Head of Cybersecurity at XYZ Government Agency highlights the organization's comprehensive approach to managing cybersecurity, emphasizing strong policies covering incident response, data protection, and access control. The effectiveness of regular cybersecurity training has significantly reduced human error related breaches, while the use of multi-factor authentication (MFA) effectively protects sensitive information. However, the organization recognizes the need for further improvement, particularly in vulnerability assessments and penetration testing, to better identify and address potential threats. Additionally, ongoing collaborations with industry leaders and government agencies are crucial in keeping the organization updated on emerging threats and best practices, ensuring a robust cybersecurity posture.

CONCLUSION

The following are the main findings that were obtained from the study on the organization's public administration organization cybersecurity policies and measures. It was also possible to identify some weaknesses in the system but all the similar factors show that the company had a good starting point in terms of cybersecurity. From this it will be possible to understand the effectiveness of the defense measures that has been done within the organization, and also make recommendations that will assist the company in boosting its defensiveness so that it can protect and keep its most private information secret. It is imperative to mention the government agencies, to which cybersecurity remains an absolute necessity. As the extent of digitization increases across the public administration organizations especially in delivering

Copyright © 2022, Journal of Public Representative and Society Provision
Under the license CC BY-SA 4.0

public services, this has exposed the organizations to increased risk of cyber warfare hence; cybersecurity must be of paramount concern. The responsibility of protecting citizens personal information lies in organizations in the public sector and may be met by developing and implementing strict cybersecurity measures, including training and education programs and periodic systematic checks, including vulnerability assessments and penetration testing. The general goal of this examination is to ensures there is an understanding of the importance of cybersecurity in public administration and to constantly explain that there needs to be an improvement and innovation in order to combat any rising threats and prevent an attack.

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

Bekkers, V. J., & Tummers, L. (Eds.). (2018). *Innovation in the public sector*. Sage. https://doi.org/10.1057/9780230307520

Bozkus Kahyaoglu, S., & Caliyurt, K. (2018). Cyber security assurance process from the internal audit perspective. *Managerial auditing journal*, *33*(4), 360-376. https://doi.org/10.1108/MAJ-02-2018-1804

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

Chowdhury, N., & Gkioulos, V. (2021). Cyber security training for critical infrastructure protection: A literature review. *Computer Science Review*, *40*, 100361. https://doi.org/10.1016/j.cosrev.2021.100361

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

Habibzadeh, H., Nussbaum, B. H., Anjomshoa, F., Kantarci, B., & Soyata, T. (2019). A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. *Sustainable Cities and Society*, *50*, 101660. https://doi.org/10.1016/j.scs.2019.101660

Hitchens, T., & Gallagher, N. W. (2019). Building confidence in the Cybersphere: a path to multilateral progress. *Journal of Cyber Policy*, *4*(1), 4-21. https://doi.org/10.1080/23738871.2019.1599032

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

Copyright © 2022, Journal of Public Representative and Society Provision
Under the license CC BY-SA 4.0

Johnson, G. A., & Vindrola-Padros, C. (2017). Rapid qualitative research methods during complex health emergencies: A systematic review of the literature. *Social Science & Medicine*, *189*, 63-75. https://doi.org/10.1016/j.socscimed.2017.07.029

Kurniawan, R., Zailani, S. H., Iranmanesh, M., & Rajagopal, P. (2017). The effects of vulnerability mitigation strategies on supply chain effectiveness: risk culture as moderator. *Supply Chain Management: An International Journal*, *22*(1), 1-15. https://doi.org/10.1108/SCM-12-2015-0482

Langheinrich, M. (2018). Privacy in Ubiquitous Computing. In *Ubiquitous computing fundamentals* (pp. 109-174). Chapman and Hall/CRC. https://doi.org/10.1201/9781420093612

Laurini, R. (2018). *Information systems for urban planning: a hypermedia cooperative approach*. Crc Press. https://doi.org/10.1201/9781315274713

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*, 13-24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Oliveira, J. B., Jin, M., Lima, R. S., Kobza, J. E., & Montevechi, J. A. B. (2019). The role of simulation and optimization methods in supply chain risk management: Performance and review standpoints. *Simulation Modelling Practice and Theory*, *92*, 17-44. https://doi.org/10.1016/j.simpat.2018.11.007

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

Redden, J. (2018). Democratic governance in an age of datafication: Lessons from mapping government discourses and practices. *Big Data & Society*, *5*(2), 2053951718809145. https://doi.org/10.1177/2053951718809145

Saura, J. R., Ribeiro-Soriano, D., & Palacios-Marqués, D. (2022). Assessing behavioral data science privacy issues in government artificial intelligence deployment. *Government Information Quarterly*, *39*(4), 101679. https://doi.org/10.1016/j.giq.2022.101679

Szczepaniuk, E. K., Szczepaniuk, H., Rokicki, T., & Klepacki, B. (2020). Information security assessment in public administration. *Computers & Security*, *90*, 101709. https://doi.org/10.1016/j.cose.2019.101709

Vitunskaite, M., He, Y., Brandstetter, T., & Janicke, H. (2019). Smart cities and cyber security: Are we there yet? A comparative study on the role of standards, third party risk management and security ownership. *Computers & Security*, *83*, 313-331. https://doi.org/10.1016/j.cose.2019.02.009

Wirtz, B. W., & Weyerer, J. C. (2017). Cyberterrorism and cyber attacks in the public sector: How public administration copes with digital threats. *International Journal of Public Administration*, *40*(13), 1085-1100. https://doi.org/10.1080/01900692.2016.1242614

Wong, L. W., Lee, V. H., Tan, G. W. H., Ooi, K. B., & Sohal, A. (2022). The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. *International Journal of Information Management*, *66*, 102520. https://doi.org/10.1016/j.ijinfomgt.2022.102520

Copyright © 2022, Journal of Public Representative and Society Provision
Under the license CC BY-SA 4.0