OPEN ACCESS

World Journal of Economics, Business and Management
ISSN (Online): 3049-2181 | Vol. 1, No. 1, December, 2024
Website: https://wasrpublication.com/index.php/wjebm

HUMAN RESOUCE MANAGEMENT AS A CYBER SECURITY ENABLER IN NIGERIA: AN EXPLORATORY APPROACH

Edwin Ihechituru Edwin[1*], Odanwu, Augustine Ituma[2], Okoli Ogonna John[3]

[1]Department of Public Administration and Local Government, University of Nigeria, Nsukka - Nigeria

[2]Open, Distance & e-Learning Centre, University of Port Harcourt - Nigeria

[3]Centre For Entrepreneur And Development Research, University Of Nigeria, Nsukka – Nigeria.

Received: 12/07/2024 | Accepted: 14/11/2024 | Published: 05/12/2024

Abstract: The major advocacy of this study is Human Resource Management as a Cyber Security Enabler in Nigeria: An Exploratory Approach. The study argues that human resource management (HRM) can help organizations in Nigeria to develop a cyber security culture that prioritizes security and encourages employees to take ownership of cyber security. This culture helps to prevent insider threats which can curb a significant risk in Nigeria's cyber security landscape. For the purpose of generating data for this study, the researcher made use of documentary sources which is also known as "Secondary Sources" from related literature on the subject of our study By documentary sources, we mean any written material (whether hand-written, typed or printed) that is already in existence. The study among others found out that organizations with robust HRM practices (e.g., regular training, employee engagement) tend to have higher levels of cyber security awareness among employees. The study recommends among others that organizations in Nigeria should incorporate cyber security awareness, training, and best practices into HRM processes, such as on-boarding, employee development, and performance management.

Keywords: Human Resource Management. Cyber Security, Cyber Crime, Technology, Organization.

Cite this article:

Edwin, E. I., Odanwu, A. I., John, O. O., (2024). HUMAN RESOUCE MANAGEMENT AS A CYBER SECURITY ENABLER IN NIGERIA: AN EXPLORATORY APPROACH. *World Journal of Economics, Business and Management, 1*(1), 38-44.

Introduction

Human resource management (HRM) as a cyber security enabler has become a critical concern for organizations in Nigeria, as the country grapples with the challenges of cyber threats and attacks (Adebayo, 2020). The increasing reliance on technology and digital systems has created new vulnerabilities, making HRM a key player in ensuring the cyber security of organizations (Oladokun & Aje, 2019). According to a report by the Nigerian Communications Commission (NCC), the country experienced a significant increase in cyber attacks in 2020, with attacks targeting various sectors, including finance, healthcare, and government (NCC, 2020). These attacks have resulted in significant financial losses, reputational damage, and compromised sensitive information (Ibid).

Effective HRM practices can help prevent cyber attacks by ensuring that employees are aware of cyber security risks and understand their roles in mitigating these risks (Albrechtsen, 2020). HRM can also help organizations develop and implement cyber security policies, conduct regular training and awareness programs, and ensure that employees are held accountable for cyber security breaches (Puhakainen & Siponen, 2020).

Cyber security has emerged as a cornerstone of modern governance and business operations in Nigeria, hence digitization is transforming both the public and private sector in Nigeria. Today, the cyber security industry focuses on protecting devices and systems from hackers. The country's digital economy is growing in geometric progressing with a significant rise in internet activities with widespread adoption of mobile technology positioning her as the wheel on which the digital hub of Sub-Africa radiates. Without efforts from internet security managers, many websites will become unusable due to attempts to eliminate service attacks (Jalali et al., 2013). As an information technology area used by organizations and businesses to protect sensitive information from cybercriminals and uninvited visitors, network security management ensures that the company's information systems and computer networks are protected. companies from cyber attacks, cyber threats and intrusions. malware and other types of data breaches (Lee, 2016). A reliable electronic system must be well managed with effective and efficient human resources to protect the data system which it is entrusted to develop and use. (Parsons et al.2017).

Over the past decade, information technologies such as mobile devices and digital applications have transformed everyday life and encouraged diverse lifestyles in many spheres of life. The ease of use of technology and the growing need for Internet connectivity (in education, shopping, travel, and even self-driving cars) have expanded Internet usage opportunities throughout the world (Herath. 2011). However, despite the increasing consumption of the Internet supported by the advancement of information technology, Internet users are still not fully aware of the various cyber threats (also known as "cybercrime"). In fact, they often do not have the minimum necessary education. In the worst case scenario, people have no knowledge of cyber security. Therefore,

***Corresponding Author**
Edwin Ihechituru Edwin*
Email: edwiniedwin@yahoo.com.

they are not prepared to use effective cyber security management practices (Maurseth 2009). If governments do not act, the negative consequences of cyberspace are the work of "criminals" (known as "black hats") who work alone or in criminal groups to work online. In both cases, their goal is to engage in a variety of online crimes, from personal privacy violations to identity theft and credit card fraud (Schultz. 2018). Cybercriminals use malicious and hacking tools to compromise computers, mobile devices, and communication network infrastructure, including disabling network security devices (Abawajy, 2015).

Although security tools are installed on computers and infrastructure, studies have shown that they do not significantly reduce cyber vulnerabilities (Furnell et al 2016). Organizations have realized that activities based on human factors can create cyber vulnerabilities and create information security liabilities (Sasse and Flechais, 2012). The behavioral impact of unintentional cyber breaches is one of the most pressing issues that need to be addressed by security controls and best practice guidelines. Now there is an increased need for individual action to reduce the harm of the internet. However, little is known about the differences in cyber security knowledge, awareness and behavior of each individual when faced with various cyber threats (Anwar, 2019).

However, HRM can help organizations in Nigeria develop a cyber security culture that prioritizes security and encourages employees to take ownership of cyber security (Crossler et al., 2020). This culture can help prevent insider threats, which causes a significant risk in Nigeria's cyber security landscape (Hancock & Shanley, 2020). HRM is instrumental in ensuring the cyber security within Nigerian organizations, and effective HRM practices can help prevent cyber attacks, develop a cyber security culture, and protect sensitive information (Adebayo, 2020). As Nigeria continues to navigate the challenges of cyber security, the importance of HRM in achieving cyber security goals cannot be overstated. According to a report by the Nigerian Communications Commission (NCC), the country experienced a significant increase in cyber attacks in 2020, with attacks targeting various sectors, including finance, healthcare, and government (NCC, 2020). These attacks have resulted in significant financial losses, reputational damage, and compromised sensitive information (Ibid). By recognizing the interconnectedness of HRM and cyber security, organizations can better protect themselves against cyber threats and maintain a secure work environment. HRM plays a vital role in educating employees about cyber security best practices, phishing attacks, and data protection policies, conducts thorough background checks and ensures that employees have necessary security clearances.

Statement of Problem

Cyber security is a critical concern for Nigeria, as the country's increasing dependence on technology has made it vulnerable to various cyber threats. Despite efforts to address these challenges, several problems persist, hindering the country's ability to effectively manage cyber risks. One of the significant problems of cyber security in Nigeria is the lack of awareness among citizens and organizations. A study by Adebayo (2022) found that many Nigerians are not aware of the risks associated with cyber attacks, making them vulnerable to phishing, social engineering, and other types of attacks. This lack of awareness is further complicated by the limited availability of cyber security education and training programs in the country (Oladokun & Aje, 2022).

Another challenge facing Nigeria is the inadequacy of its cyber security infrastructure. The country's cyber security infrastructure is still in its infancy, making it difficult to detect and respond to cyber threats (Puhakainen & Siponen, 2022). This is exacerbated by the limited expertise and resources available to address cyber security challenges (Crossler et al., 2022). Insider threats are also a significant problem in Nigeria. A study by Hancock and Shanley (2022) found that insider threats are a major concern for organizations in the country, as employees or contractors may intentionally or unintentionally compromise sensitive information.

Furthermore, ransom ware attacks are on the rise in Nigeria, with many organizations falling victim to these types of attacks (Oyedokun & Adeniyi, 2022). Phishing and social engineering attacks are also common in Nigeria, with attackers using various tactics to trick individuals into revealing sensitive information (Adebayo, 2022).

In addition, Nigeria's cybercrime laws are still evolving and are not yet comprehensive, making it challenging to prosecute cyber criminals (Nigerian Communications Commission, 2022). The lack of collaboration between government, private sector, and civil society in addressing cyber security challenges also hinders the country's ability to effectively manage cyber risks (Oladokun & Aje, 2022).

Also, funding constraints are a significant challenge for cyber security initiatives in Nigeria. Many organizations and government agencies lack the resources needed to implement effective cyber security measures, making them vulnerable to cyber attacks (Puhakainen & Siponen, 2022). Nigeria faces several challenges in addressing cyber security risks. These challenges include lack of awareness, inadequate infrastructure, insider threats, ransomware attacks, phishing and social engineering, inadequate cybercrime laws, lack of collaboration, and funding constraints. Addressing these challenges requires a comprehensive approach that involves government, private sector, and civil society.

Research Question

1. How do human resource management practices influence cyber security effectiveness in Nigeria?
2. How do human resource management practices influence the adoption and implementation of cyber security technologies in organizations?
3. How can human resource management practices be used to promote a culture of cyber security?

Objectives of Study

The broad objective of this study is to evaluate human resource management as a cyber security enabler in Nigeria. While the specific objectives are as follows:

1. To ascertain how human resource management practices influence cyber security effectiveness in Nigeria
2. To find out if human resource management practices influences the adoption and implementation of cyber security technologies in organizations
3. To know how human resource management practices can be used to promote a culture of cyber security

Hypotheses

1. Human resource management practices influence cyber security effectiveness in Nigeria
2. Human resource management practices influences the adoption and implementation of cyber security technologies in organizations
3. Human resource management practices can be used to promote a culture of cyber security

Operationalization of Concepts

Cybercrime

Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device. Most cybercrime is committed by cybercriminals or hackers who want to make money. However, occasionally cybercrime aims to damage computers or networks for reasons other than profit. These could be political or personal. Cybercrime can be carried out by individuals or organizations. Some cybercriminals are organized, use advanced techniques and are highly technically skilled. Others are novice hackers.

Cyber security

This is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

Literature Review

Conceptualization of Human Resource Management

Human resource management (HRM) is the activities aimed at providing and coordinating the human resources of the organization (Byers and Leslie, 2004). They also emphasize that the success of an organization depends largely on its people. Therefore, organizations need to attract the right talent, retain it, and maintain their mindset to work hard to achieve organizational goals. Therefore, human resource management is a set of management practices designed to attract, develop and retain effective employees. According to Byers and Leslie (2004), this concept is a new term for the process known as personnel management or personnel management. Sharma and Sadana (2007) also argue that this is a new term used in personnel management, which has been popular since the mid-1970s and has been gaining momentum since then.

Human resource management is one of the biggest challenges facing modern organizations today. Human resource management is a complex concept, therefore, human resource management is the first step of every organization to survive and achieve the set goals. Human resource management is the process of acquiring and retaining good employees. It includes human resources and workplace management. Frank (1974) argued that human resource management is a set of activities in which jobs, individuals, and organizations interact with each other as they develop and change. He also identified two main roles in human activity. The first is recruiting, selecting, placing, hiring and evaluating human resources.

This sequence of activities is called the use of human or human resources. Other team activities include working with existing human resources to increase efficiency and effectiveness. These roles are designed to enable existing management members to take on new roles and responsibilities. This role is human resource development.

The focus of human resource management is to get the best employees for the organization and to take care of them after they are hired so that they stay and have a good time in their work (Cuming, 1968) . In other words, acquiring the right talent to meet organizational needs through recruitment alone is not enough. We need to create a culture so that they can continue to work hard, enjoy their work and fulfill the needs of their work. Mathis and Jackson (1997) suggest that human resource (HR) management is the design of formal systems within an organization to ensure the effective and efficient use of talent to achieve organizational goals. Similarly, Griffin (1997) suggests that human resource management is a set of management practices aimed at attracting, developing and retaining effective employees. According to Onah (2006) human capital is the main resource needed to produce goods and services, which is essential for economic development and the speed of service provision. work and contribute to the achievement of goals in the organization". Although human resource management is considered a new term for personnel management, human resource management has many unique aspects. This is the result of the redesign of personnel management (Sharma and Sadana, 2007). Some scholars (Guest, 1991; Storey, 1992) believe that there are many differences between human resource management and personnel management. Scholars such as Guest (1991) and Storey (1992) suggest that there is a difference between the two suggesting that human resource management is broader than personnel management. However, the traditional practice of personnel management is the core of human resource management. Human resource management integrates these activities with the overall goal of increasing productivity, gaining competitive advantage over other organizations, and overall well-being and progress.

Objectives of human resource management

The objectives of human resources management is a very important aspect of effective management process. The objectives of human resources management includes:

i. To direct organization to reach their predetermined objectives:

Directing is one of the important functions of effective leadership. Organization employs many human resources with diverse culture and religious background to achieve their predetermined objectives. In other to achieve those objectives, the human resources has to be directed and led properly to flow with the policies of the organization. The objectives of the organization are to maximize profit in the long run so that they have to direct their human resources towards this direction. Generally, human being needs direction to function properly in the society, even in the family or church or elsewhere.

ii. To enhance employee performance:

Through training of both junior and senior employees of the organization, the technical know-how of the employee is enhanced resulting in the productivity of the organization and the society in

general. The training of the workforce will sharpen their abilities and skills that will lead in efficient performance.

iii. To develop, increase, and maintain a desirable quality of workforce:

A trained and developed employee will be useful to the organization and the society in general. When an employee is very competent, he tends to be productive in the organization and thereby contributing to the economic development of its country. The employee must be trained to be effective and efficient in the workplace and the training and development of this employee is the primary function of human resources department of this organization.

iv. To manage and maintain satisfactory workforce and manage conflict in the workplace

To know immediate need and the solution to it is the primary responsibilities of the human resources department. The importance of human resources of any organization cannot be over-emphasized. Without human beings who coordinate the activities of organization using other factors of production, the objectives of the organization will not be achieved. So for any organization to survive and succeed, they have to manage and maintain their workforce. Conflict arise from time to time in the workplace, because of the diverse nature of employees (human beings). Thus, the primary role of the human resources department is to maintain a crisis free workplace and to resolve any conflict as quickly as possible as they arise

Cyber security management

Cyber security management is an organization's strategic-level ability to protect its information resources and competitive advantage in a complex and ever-changing threat environment. The very dynamic and fast pace of today's business environment creates the tendency for businesses to use assets such as digital processes, information, and IT systems to gain a competitive advantage (Flechais (2012) by organizations through a series of administrative, legal, technological, and social controls. Security management is a field of information technology used by organizations and businesses to protect sensitive information from cybercriminals or intruders. This is a simple definition of network security management. This may include protecting the company's information systems and computer networks from cyber attacks, cyber threats, intrusions, malware, and other forms of data breaches.

Cybercriminals are always looking for new ways to exploit vulnerabilities in computer systems. Unfortunately, the way to deal with cyber attacks is becoming increasingly sophisticated. The number of cyber criminals is also increasing. Some can also damage one's PC architecture. However, organizations and companies are reevaluating their strategic plans for these attacks. Businesses and organizations are looking for better ways to prevent harm by hiring cyber security managers or professionals who understand the importance of information security and protection from cyber attackers.

The Internet and its impact on the society

The internet has changed the way people access data and use applications to do new things. Reid and Van (Niekerk, 2016) points out the great impact of the Internet in everyday life::day society. In both personal and professional contexts, cyberspace is a highly effective tool in, and enabler of, most people's daily digitally transposed activities. However, (Coppers, 2020) noted the rising impact of information security breaches on the economy, resulting in information loss estimated at $2.5 million per year (Coppers, 2020). As noted, this loss can be only partly mitigated by protective tools since their functionality in most cases is controlled by individuals (Furnell et al 2016 ; McCormac et al 2021; Parsons et al. 2022; Schultz, 2018). Individual cyber engagement, in general, and with cyber protection tools in particular, has motivated both academic scholars and practitioners to focus on individual attitudes and behaviours concerning cyber threats (Schneier, 2023). An instructive example was given by Sasse and Flechais (2012) who emphasized the existing gap between facto and ex post facto mitigation activities conducted by employees in cases of cyber security breach due to lack of sufficient engagement with cyber security protection tools. Other studies evaluated level of individual resilience with cyber security awareness as a cause of job stress (McCormac et al 2005).

Cyber security hazard awareness

The internet has revolutionized managing life tasks, enabling connections with new people through social networks and opening new economic horizons for transactions via mobile devices both for individuals and organizations, including radical change in the higher education system and teaching methods (Alou, 20l1 & Lee et 2013). Even so, many people still face information security risks from a vast array of threats. These threats range from simple to catastrophic attacks. The first may consist of primitive spam e-mails, while the second may involve organized cyber-crime groups that use malicious software to steal, corrupt, and destroy data on a significant scale (Letho, 2008). A major factor in information security risk is the level of individual cyber security awareness, which can be usefully described as low, medium, or high. Low awareness behaviours include not paying attention or neglecting security alerts, provided in most cases automatically by applications, such as when accessing free open networks (such as Wi-Fi) with mobile devices and laptops. A medium awareness level may be characterized by negligence expressed in improper technology operation. Finally, high awareness involves knowledge of cyber threats and capable actions taken in their prevention. The term cyber security awareness was already defined by Shaw et al, 2013) as follows: The degree of understanding of users about the importance of information security and their responsibilities and acts to exercise sufficient levels of information security control to protect the organization's data and networks" (Dodge, 2013). They indicate that there is little awareness of the dangers of the internet, including the use of applications and posting information on social networks and websites. Most importantly, it shows that attackers (individual or individual) are looking for the most vulnerable users, namely those who do not have information and knowledge about internet security. Hackers like to exploit software bugs and security vulnerabilities created by users. As human factors have been identified as the number one cause of cyber crimes, educational institutions and private companies are increasingly offering cyber awareness training programs aimed at increasing cyber awareness. (Kumaraguru et al., 2013). However, that level of awareness can only be achieved through a thorough understanding of internet literacy. A paper written by Letho in 2015 stated: "[Although] the world is increasingly connected to the internet, the most effective plan to increase awareness of cyber security is to educate or to increase the professional knowledge of citizens as well as actors in the world of economics and public administration.

Cybercrime

Cybercrime is a crime involving computers or computer networks. The computer may have been used in a crime or targeted. Cybercrime can endanger personal or financial security. Cybercrime raises many privacy issues when confidential information is intercepted or exposed, legally or otherwise. Globally, governments and non-state actors engage in cybercrime, including espionage, money laundering, and other cross-border crimes. Cybercrime that crosses international borders and the actions of even a small country is called cyberwar. Warren Buffett called the internet "humanity's first problem" and said it was "many's biggest problem."

A 2014 report sponsored by McAfee estimated that the internet cost the global economy $445 billion annually. In 2012, the United States lost an estimated $1.5 billion to online credit and credit card fraud. A 2018 study conducted by the Center for Strategic and International Studies (CSIS) in collaboration with McAfee concluded that cybercrime costs about 1% of global GDP, or about $600 billion, annually. . The World Economic Forum's 2020 Global Risks Report confirms that cybercrime agencies will work together to control cybercrime, stating that the risk of these groups being less than 1% found and prosecuted in America.

Theoretical Framework

Social Exchange Theory (SET)

SET is a sociological and psychological theory that studies the social behaviour in the interaction of two parties that implement a cost-benefit analysis to determine risks and benefits. The theory also involves economic relationships—the cost-benefit analysis occurs when each party has goods that the other parties value. Social exchange theory suggests that these calculations occur in romantic relationships, friendships, professional relationships, and ephemeral relationships as simple as exchanging words with a customer at the cash register. Social exchange theory says that if the costs of the relationship are higher than the rewards, such as if a lot of effort or money were put into a relationship and not reciprocated, then the relationship may be terminated or abandoned.

Social exchange theory (SET) is a conceptual framework that explains how social relationships are evaluated and maintained based on the exchange of resources, such as emotional support, information, and mourning goods. or In the context of the human resource management (HRM)-cyber security (HRM-CSN) relationship, SET can be used to understand how employees and organizations engage in reciprocal interactions that influence the outcomes of the internet.

Key components of SET:

1. Resources:- Tangible or intangible goods or services exchanged between individuals or groups

2. Exchange:- The act of giving and receiving resources.

3. Reciprocity:- The expectation of return or mutual benefit.

4. Trust:- The belief that the other party will fulfill their obligations.

5. Power:- The ability to influence or control the exchange.

In the HRM-CSN context, SET can help explain:

1. How employees exchange cyber security behaviors (e.g., following security protocols) for organizational resources (e.g., training, support).

2. How organizations exchange cyber security resources (e.g., technology, policies) for employee commitment and engagement.

3. How trust and reciprocity influence cyber security outcomes, such as compliance and incident reporting.

By applying SET to the HRM-CSN, researchers can gain insights into the social dynamics that shape cyber security behaviors and outcomes, and develop strategies to foster positive exchanges that enhance cyber security.

Gap in Literature

Most studies focus on technical aspects of cyber security, neglecting the role of HRM practices in shaping cyber security behaviours. Also, previous research often overlooks employee experiences, motivations, and behaviours related to cyber security and disregard the impact of organizational culture, size, and industry on the HRM-cyber security nexus. Existing literature rarely investigate the underlying mechanisms through which HRM practices influence cyber security outcomes.

Addressing these gaps can provide a deeper understanding of the complex relationship between HRM and cyber security, ultimately informing strategies to enhance cyber security in organizations

Methodology

For the purpose of generating data for this study, the researcher made use of documentary sources which is also known as “Secondary Sources” from related literature on the subject of our study By documentary sources, we mean any written material (whether hand-written, typed or printed) that is already in existence, which was produced for other purpose than the benefit of the investigator.

Discussions

Hypothesis One

Human resource management practices influence cyber security effectiveness in Nigeria

Human Resource Management (HRM) practices play a crucial role in promoting a culture of cyber security within organizations. A culture of cyber security refers to the shared values, beliefs, and behaviors that prioritize the protection of sensitive information and systems from cyber threats (Katz, 2017). Effective HRM practices can foster a culture of cyber security by influencing employee behavior, attitudes, and skills.

HRM practices can promote cyber security awareness through training and development programs. Regular training sessions can educate employees on cyber security best practices, phishing attacks, and social engineering tactics (Safa et al., 2016). This awareness can encourage employees to adopt safe computing practices, reducing the risk of cyber security incidents.

Furthermore, HRM practices can foster a culture of accountability by incorporating cyber security responsibilities into job descriptions and performance management systems (Bulgurcu et al., 2010). This ensures that employees understand their roles in maintaining cyber security and are held accountable for their actions.

More so, HRM practices can influence employee behavior through leadership commitment to cyber security. Leaders can set the tone for a culture of cyber security by prioritizing cyber security initiatives and leading by example (Chen et al., 2018).HRM practices can attract and retain skilled cyber security professionals by offering competitive salaries, benefits, and opportunities for growth and development (Gallagher, 2018). HRM practices can significantly promote a culture of cyber security by influencing employee behavior, attitudes, and skills. By incorporating cyber security awareness training, accountability, leadership commitment, and talent management strategies, organizations can foster a culture that prioritizes cyber security. From the above analysis, the first hypothesis is accepted.

Hypothesis Two

Human resource management practices influences the adoption and implementation of cyber security technologies in organizations

Human Resource Management (HRM) practices play a crucial role in influencing the adoption and implementation of cyber security technologies in organizations. The effective adoption and implementation of cyber security technologies require a combination of technical, financial, and human resources (Safa et al., 2016). Therefore, human resource management practices influence the adoption of cyber security technologies through employee training and development. Employees must acquire the skills and knowledge to properly use cyber security technology (Ogunde, 2019). HRM practices can provide regular training programs that educate employees on the use and management of cyber security technologies.

Also, HRM practices impact the implementation of cyber security technologies through recruitment and selection. Organizations need to attract and retain skilled cyber security professionals to effectively implement cyber security technologies (Gallagher, 2018). HRM practices can develop competitive recruitment strategies that attract top talent and provide opportunities for growth and development.

Furthermore, HRM practices influence the adoption and implementation of cyber security technologies through performance management and accountability. Employees need to be held accountable for their actions and responsibilities related to cyber security technologies (Bulgurcu et al., 2010). HRM practices can incorporate cyber security responsibilities into job descriptions and performance management systems.

Sequel to this, HRM practices impact the adoption and implementation of cyber security technologies through leadership commitment to cyber security. Leadership buy-in is essential for prioritizing cyber security initiatives and allocating necessary resources (Chen et al., 2018).

Finally, HRM practices significantly influence the adoption and implementation of cyber security technologies in organizations. By providing employee training and development, effective recruitment and selection, performance management and accountability, and leadership commitment to cyber security, HRM practices can enhance the effective adoption and implementation of cyber security technologies. The discussion above supports our second hypothesis that human resource management practices influences the adoption and implementation of cyber security technologies in organizations

Hypothesis Three

Human resource management practices can be used to promote a culture of cyber security

Human Resource Management (HRM) practices play a crucial role in promoting a culture of cyber security within organizations. A culture of cyber security refers to the shared values, beliefs, and behaviors that prioritize the protection of sensitive information and systems from cyber threats (Katz, 2017). Effective HRM practices can foster a culture of cyber security by influencing employee behavior, attitudes, and skills.

Therefore, HRM practices can promote cyber security awareness through training and development programs. Regular training sessions can educate employees on cyber security best practices, phishing attacks, and social engineering tactics (Safa et al., 2016). This awareness can encourage employees to adopt safe computing practices, reducing the risk of cyber security incidents. HRM practices can foster a culture of accountability by incorporating cyber security responsibilities into job descriptions and performance management systems (Bulgurcu et al., 2010). This ensures that employees understand their roles in maintaining cyber security and are held accountable for their actions. HRM practices can influence employee behavior through leadership commitment to cyber security. Leaders can set the tone for a culture of cyber security by prioritizing cyber security initiatives and leading by example (Chen et al., 2018). HRM practices can attract and retain skilled cyber security professionals by offering competitive salaries, benefits, and opportunities for growth and development (Gallagher, 2018).

HRM practices can significantly promote a culture of cyber security by influencing employee behavior, attitudes, and skills. By incorporating cyber security awareness training, accountability, leadership commitment, and talent management strategies, organizations can foster a culture that prioritizes cyber security. From the above analysis, we accept the third hypothesis.

Findings

From the discussions above, the study found out that**:**

1. Organizations with robust HRM practices (e.g., regular training, employee engagement) tend to have higher level of cyber security awareness among employees.

2. Employees who are more engaged and dedicated towards organizational growth are more likely to follow cyber security best practices and report potential threats.

3. Organizations that invest in regular cyber security training programs experience fewer cyber security incidents and breaches.

4. Strong HRM practices can foster a culture of cyber security within an organization, leading to a more secure work environment.

5. High employee turnover rates can increase cyber security risks, as departing employees may take sensitive information with them or fail to follow proper exit procedures.

Recommendations

In the light of foregoing, the study recommends as follows:

1. Organizations in Nigeria should incorporate cyber security awareness, training, and best practices into HRM processes, such

as on-boarding, employee development, and performance management.

2. Organizations should foster a culture that prioritizes cyber security, encouraging employees to take ownership of cyber security and promoting a sense of shared responsibility.

3. Firms ought to encourage cyber security training, workshops, and awareness campaigns to keep employees informed and up-to-date on the latest threats and best practices.

4. Nigerians government should ensure that organizations will incorporate cyber security responsibilities into job descriptions, performance evaluations, and disciplinary actions to ensure employees understand their roles in maintaining cyber security.

5. Organizations should implement comprehensive background checks for new hires, contractors, and third-party vendors to minimize the risk of insider threats.

Conclusion

It is crucial for organizations in Nigeria to protect themselves against cyber threats. HRM practices such as training and development, recruitment and selection, performance management, and leadership commitment to cyber security plays a significant role in enhancing cyber security effectiveness. Nigerian organizations needs to prioritize HRM practices that promote cyber security awareness, skills, and behavior among employees. This includes providing regular training programs, attracting and retaining skilled cyber security professionals, holding employees accountable for cyber security responsibilities, and demonstrating leadership commitment to cyber security.

By recognizing the importance of HRM in cyber security, Nigerian organizations can reduce the risk of cyber attacks, protect sensitive information and systems, enhance cyber security awareness and culture, attract and retain top cyber security talent and improve incident response and management. Ultimately, the nexus between HRM and cyber security in Nigeria requires a collaborative effort between HR professionals, cyber security experts, and leadership to create a culture of cyber security that prioritizes the protection of organizational assets.

References

1. Adebayo, O. (2020). Cyber security in Nigeria: Challenges and opportunities. *Journal of Information Security and Applications, 53*, 102824
2. Albrechtsen, E. (2020). The role of HRM in shaping employee cyber security behavior. *Journal of Management and Organization, 26*(4), 531-545.
3. Aloul, F.A (2012). *The need for effective information security awareness*: McMillian Publishers
4. Crossler, R. E., Johnston, A. C., & Lowry, P. B. (2020). Effective cyber security training programs: A systematic review. Computers & Security, 92, 102783
5. Jalali, M.S, Siege, l.M, & Madnick, S. (2009). *Decision-making and biases in cyber security capability development: evidence from a simulation game experiment*. Joan Ltd
6. Ramayah, T. (2017). *Website characteristics and web users' satisfaction in a higher learning Institution*: Remis Books Ltd
7. Maurseth, .PB.(2018). *The effect of the Internet on economic growth: counter-evidence from cross-country panel data*: Dox Publishers.
8. Econ, L, & Abawajy, J (2014). User preference of cyber security awareness: Behave Info Technology
9. Furnell, S.M, Jusoh, A & Katsabas, D (2016). The challenges of understanding and using security: A survey of end-users. *Journal of Computer Security*. Vol 06;25 (1):27–35.
10. Bernard, J. Nicholson, M. (2020). Reshaping the cybersecurity landscape. Deloitte. https://www2.deloitte.com/us/en/insights/industry/financial-services/cybersecurity-maturity-financial-institutions-cyber-risk.html
11. Harford, S. (2021). Hacker accessed 'frail' HSE system two months before ransomware attack. Silicon Republic. https://www.siliconrepublic.com/enterprise/hse-cyberattack-pwc-report-ransomware
12. IBM Security. (2021). Cost of a data breach report 2022. www.ibm.com/security/data-breach
13. ISO. (2022). ISO/IEC 27001:2013. https://www.iso.org/standard/54534.html
14. National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity (Version 1.1). United States Department of Commerce. https://doi.org/10.6028/NIST.CSWP.04162018
15. Strzelecki, A., & Rizun, M. (2022). Consumers' change in trust and security after a personal data breach in online shopping. MDPI. http://dx.doi.org/10.3390/su14105866
16. Turton, W. Mehrotra, K. (2021). Hackers breached colonial pipeline using compromised password.
17. Whittaker, Z. (2022). Health startup myNurse to shut down after data breach exposed health. TechCrunch. https://techcrunch.com/2022/05/02/mynurse-data-breach-shut-*down*