International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Field Study on the Impact of the Level of Knowledge of Human Resources Employees About the Principles and Applications of Cybersecurity on Human Resources Laws, Between the Theoretical Aspect and the Practical Application Reality

Mohamad A S Alenzi[1*], Mr. Maher Ali Rusho[2]

Submitted: 03/02/2024 **Revised**: 11/03/2024 **Accepted**: 17/03/2024

Abstract: As organizations become more aware of the extensive damage caused by cyber threats, the need for effective cybersecurity measures has intensified. In parallel with this, Human Resources departments are tasked with legal compliance and safeguarding sensitive employee information. However, there appears to be a gap between cybersecurity understanding and HR legal compliance, leaving organizations vulnerable to potential breaches and regulatory penalties. In this article, we delve into the intricate relationship between cybersecurity understanding and HR legal compliance. As, we investigate how a lack of cybersecurity knowledge within HR departments can hinder compliance efforts, and conversely, how a strong understanding of cybersecurity can help HR personnel identify and mitigate potential risks. By bridging this gap, organizations can create a more holistic approach to cybersecurity and ensure legal compliance.

Keywords: *Culture, Cyber-security, department, employee, organization, Human Resources,*

Introduction

Human Resources (HR) plays in promoting and maintaining a robust cybersecurity culture within an organization. HR Indeed has a crucial role in cybersecurity, especially in educating and empowering employees to protect the organization's digital assets. It serves as a vital resource for employees when it comes to cybersecurity. They are often the first point of contact for employees seeking information or assistance related to cybersecurity issues. Moreover, HR plays a pivotal role in shaping and nurturing a strong cybersecurity culture within the organization. HR's involvement in cybersecurity has grown significantly because it is now widely recognized that providing cybersecurity training to employees is essential. New employees should receive information on practicing good cybersecurity hygiene as part of their onboarding process. This training helps boost their confidence when facing cybersecurity threats [1-3]. Cybersecurity training should include guidance on recognizing and dealing with common threats like phishing attacks and password security. Employees need to know how to identify these threats and take appropriate action to mitigate them. HR should also educate employees about the organization's digital transformation efforts and the implementation of new technologies. Understanding the security implications of these changes is crucial to maintaining cybersecurity. It should provide guidelines and best practices for employees who use their personal devices for work purposes. This includes ensuring that these devices are secure and don't pose risks to the organization's data. HR should train employees on secure remote access protocols, especially if remote work is a part of the organization's culture [4]. Additionally, they should educate employees about business continuity plans and how to respond in case of incidents. Employees should be aware of the incident response and recovery procedures within the organization. HR can play a role in educating them on these processes and their responsibilities during a cybersecurity incident. HR can communicate and enforce policies regarding the use of company-issued and personal devices in the workplace [5-9]. This ensures that employees follow security guidelines. In cybersecurity training and awareness is critical for building a strong cybersecurity culture within an organization. It not only helps employees protect the organization from cyber threats but also instills confidence and preparedness among employees to handle cybersecurity incidents effectively. The growth in internet technology and mobile applications has led to increasingly complex and sophisticated cyber threats [10-11]. Attackers are continually evolving their methods, making it challenging for organizations to defend against cyber-attacks effectively. Organizations have deployed various security measures, including password management, data leak prevention, content monitoring technologies, and firewalls. These tools provide technical

[1*] *PHD in Business Management, Green Human Resource Management, Community College of Qatar,*
Email: Mohamad.alenzi@ccq.edu.qa, ORCID:0000-0002-6063-5644
[2] *Specialized Program Grad Student, Lockheed Martin Performance-Based Master of Engineering in Engineering Management (ME-EM) Degree Program, University of Colorado Boulder, maher.rusho@colorado.edu (or maru4732@colorado.edu)*

solutions for protecting data and information systems, particularly at the network perimeter. Despite advanced security technologies, the human factor remains a significant vulnerability. Some employees may not fully comply with their organization's information security policies [12-15]. This can result from negligence or a lack of awareness regarding security risks. Insider threats, both intentional and unintentional, are a major concern. Employees may leak valuable data either deliberately or accidentally, posing a serious risk to an organization's cybersecurity. Research suggests that security policies don't always work effectively for employees. Some employees may not take these policies seriously or may underestimate the associated risks. Even employees who receive information security training may not always exhibit the expected cybersecurity behavior. Organizations invest significant resources in cybersecurity to protect their critical data and systems. They expect a positive ROI on these investments, meaning they anticipate a reduction in cyber risks and potential losses as a result of their security efforts. The multifaceted nature of cybersecurity challenges. While technical solutions are important, addressing human behavior and awareness, as well as evaluating the effectiveness of security policies and training programs, are crucial elements in achieving comprehensive cybersecurity. Organizations must continually adapt their cybersecurity strategies to stay ahead of evolving cyber threats and maximize the return on their cybersecurity investments [16-19].

The importance of cybersecurity in HR legal compliance

Ensuring legal compliance is a critical responsibility for Human Resources departments. From maintaining employee records to handling sensitive information, HR professionals play a crucial role in safeguarding data and ensuring privacy. With the increasing number of cyber threats targeting organizations, it is imperative for HR departments to have a solid understanding of cybersecurity principles and practices. Cybersecurity is no longer just an IT issue; it is a business imperative. HR departments are not immune to cyber threats, as they often hold a treasure trove of sensitive employee data, including social security numbers, bank account details, and medical information. Failure to protect this data can lead to severe consequences, both in terms of financial losses and damage to the organization's reputation. To effectively address these risks, HR professionals need to be equipped with the knowledge and skills necessary to identify and mitigate cybersecurity threats. By integrating cybersecurity principles into their compliance efforts, HR departments can play a pivotal role in ensuring the organization's overall security posture.

Cybersecurity threats and their impact on HR legal compliance

The landscape of cyber threats is constantly evolving, and organizations must adapt their cybersecurity strategies accordingly. Employee data is a prime target for cybercriminals, as it can be sold on the dark web, used for identity theft, or exploited for financial gain. HR departments, holding a wealth of personal information, are at the forefront of this battle against cyber threats.One of the most common cybersecurity threats faced by HR departments is phishing attacks. These attacks involve cybercriminals sending deceptive emails or messages to employees, tricking them into revealing sensitive information or clicking on malicious links. The consequences of a successful phishing attack can be devastating, as it can lead to unauthorized access to employee records or even compromise the entire network. Another significant threat to HR departments is ransomware attacks. Ransomware is a type of malware that encrypts an organization's data, rendering it inaccessible until a ransom is paid. HR departments, with their valuable employee information, are prime targets for these attacks. Failure to protect against ransomware can result in significant financial losses and potential legal repercussions. The impact of these cybersecurity threats on HR legal compliance cannot be understated. A breach of employee data can lead to violations of privacy laws, such as the General Data Protection Regulation (GDPR) or the EU General Data Protection Regulation (GDPR). These regulations impose strict requirements on organizations regarding the collection, storage, and protection of personal data. Non-compliance can result in substantial fines and reputational damage.

Bridging the gap: *Enhancing cybersecurity understanding within HR departments*

To bridge the gap between cybersecurity understanding and HR legal compliance, organizations must invest in training and education programs for HR professionals. By equipping HR personnel with the necessary knowledge and skills, organizations can empower them to identify and mitigate potential cybersecurity risks effectively. Training programs should focus on raising awareness about common cyber threats, such as phishing and ransomware. HR professionals should be educated on how to recognize and report suspicious emails or messages, as well as the importance of maintaining strong passwords and implementing multi-factor authentication. Additionally, they should be trained on the proper handling and protection of employee data, ensuring compliance with relevant privacy regulations. Education programs should also cover emerging cybersecurity trends and best practices. HR professionals should be kept up to date with the latest security technologies and tools, enabling them to make informed decisions when implementing cybersecurity measures within their departments. By staying knowledgeable about the evolving threat landscape, HR personnel can proactively identify vulnerabilities and implement appropriate countermeasures.

Implementing cybersecurity policies and procedures in HR departments

In addition to training and education, organizations should establish clear cybersecurity policies and procedures within their HR departments. These policies should outline the expectations and responsibilities of HR professionals regarding data protection and compliance. By providing a framework for cybersecurity practices, organizations can ensure consistency and adherence to best practices across the HR department. Cybersecurity policies should address key areas such as data classification, access controls, incident response, and employee awareness. Data classification involves categorizing employee data based on its sensitivity and defining appropriate security controls for each category. Access controls ensure that only authorized personnel have access to sensitive information, reducing the risk of unauthorized disclosure or misuse. Incident response procedures are crucial for effectively managing cybersecurity incidents within HR departments. HR professionals should be trained on how to respond to a data breach or a cyber attack, including notifying affected individuals, communicating with regulatory authorities, and implementing remediation measures. By having a well-defined incident response plan, HR departments can minimize the impact of cybersecurity incidents and ensure compliance with legal requirements. Employee awareness is a vital component of any cybersecurity strategy. HR departments should implement regular awareness programs to educate employees about the importance of cybersecurity and their role in maintaining the organization's security posture. This can include training sessions, newsletters, and simulated phishing exercises to test employee readiness and reinforce best practices.

The role of HR in ensuring legal compliance in cybersecurity

HR departments play a critical role in ensuring legal compliance in cybersecurity. By integrating cybersecurity principles and practices into their daily operations, HR professionals can contribute to the organization's overall security posture and protect sensitive employee data. One of the key responsibilities of HR professionals is to create a culture of security within the organization. This involves promoting cybersecurity awareness among employees, encouraging the adoption of best practices, and fostering a proactive approach to data protection. HR departments can achieve this by incorporating cybersecurity training and awareness programs into employee onboarding processes and ongoing professional development initiatives. HR professionals also have a vital role in ensuring compliance with privacy regulations. They should collaborate with legal and IT departments to understand the requirements imposed by relevant regulations, such as the GDPR or EU-GDPR. By aligning their practices with these regulations, HR departments can minimize the risk of non-compliance and the potential financial and reputational consequences that accompany it. Additionally, HR professionals should establish strong relationships with cybersecurity teams and IT departments. By fostering collaboration and communication, HR professionals can contribute to the development and implementation of effective cybersecurity measures. This partnership ensures that HR legal compliance efforts align with the organization's overall cybersecurity strategy, resulting in a more robust and resilient security posture.

Case studies: ***Examples of successful integration of cybersecurity and HR legal compliance***

Several organizations have successfully bridged the gap between cybersecurity understanding and HR legal compliance, resulting in improved security and compliance outcomes. These case studies provide valuable insights into the strategies and best practices that organizations can adopt to enhance collaboration between cybersecurity and HR teams.

Case Study 1: XYZ Corporation

XYZ Corporation recognized the need to strengthen its cybersecurity measures and improve HR legal compliance. The organization implemented a comprehensive training program for HR professionals, covering topics such as cybersecurity awareness, data protection, and incident response. By investing in employee education, XYZ Corporation empowered HR personnel to identify and mitigate potential risks effectively. This resulted in improved compliance with privacy regulations and a significant reduction in security incidents.

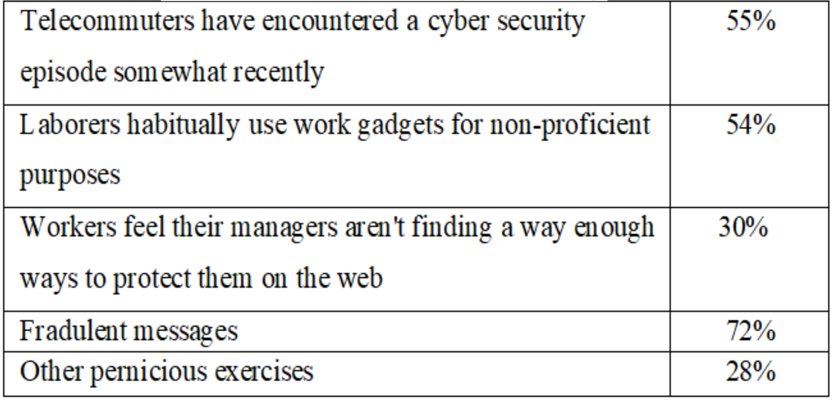
Case Study 2: ABC Corporation

ABC Corporation faced challenges in aligning cybersecurity and HR legal compliance efforts. To address this, the organization established a cross-functional working group comprising representatives from HR, legal, and IT departments. This collaborative approach facilitated the sharing of knowledge and expertise, enabling the development of robust cybersecurity policies and procedures. By leveraging the collective strengths of different departments, ABC

Corporation achieved a more holistic approach to cybersecurity and improved compliance outcomes.

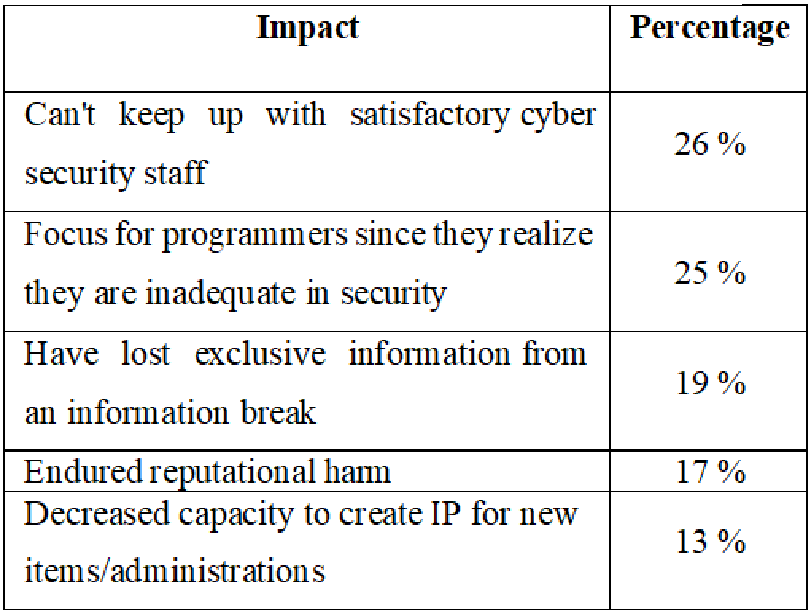
Analysis Part of the Study

Table 1: *HR needs about Cyber security*



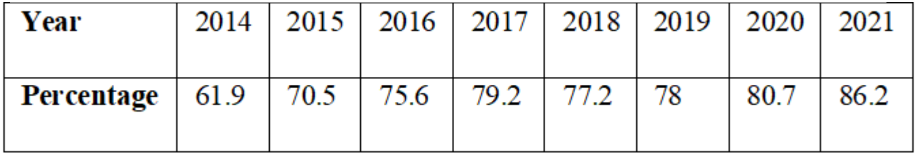
Telecommuters have encountered a cyber security episode somewhat recently	55%
Laborers habitually use work gadgets for non-proficient purposes	54%
Workers feel their managers aren't finding a way enough ways to protect them on the web	30%
Fradulent messages	72%
Other pernicious exercises	28%

Table 2: *Impact of Cyber security Workforce Shortage*



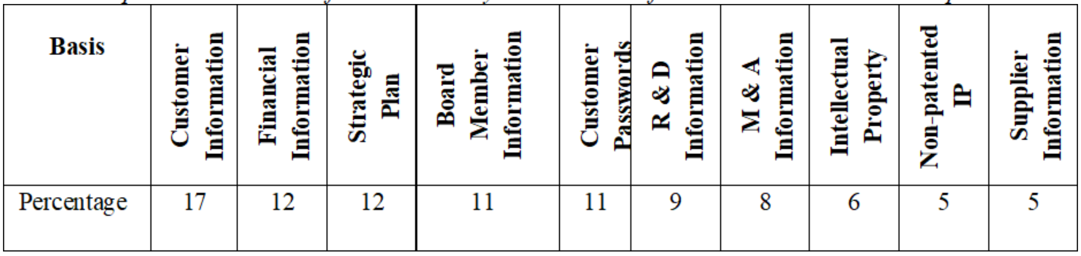
Impact	Percentage
Can't keep up with satisfactory cyber security staff	26 %
Focus for programmers since they realize they are inadequate in security	25 %
Have lost exclusive information from an information break	19 %
Endured reputational harm	17 %
Decreased capacity to create IP for new items/administrations	13 %

Table 3: *Percentage of Organizations compromised by at least one Successful Cyber Attack*



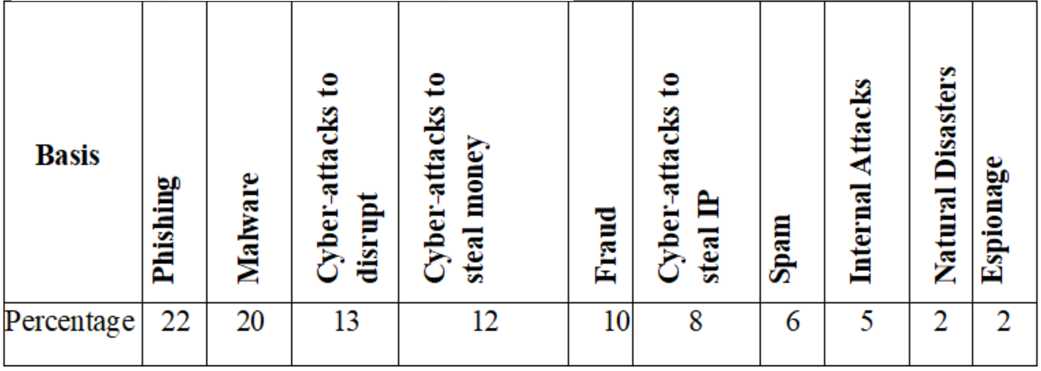
Year	2014	2015	2016	2017	2018	2019	2020	2021
Percentage	61.9	70.5	75.6	79.2	77.2	78	80.7	86.2

Table 4:*Top Most Valuable Information to Cyber Criminals from Human Resource Perspective*



Basis	**Customer Information**	**Financial Information**	**Strategic Plan**	**Board Member Information**	**Customer Passwords**	**R & D Information**	**M & A Information**	**Intellectual Property**	**Non-patented IP**	**Supplier Information**
Percentage	17	12	12	11	11	9	8	6	5	5

Table 5:*Biggest Cyber threats to organizations*



Basis	Phishing	Malware	Cyber-attacks to disrupt	Cyber-attacks to steal money	Fraud	Cyber-attacks to steal IP	Spam	Internal Attacks	Natural Disasters	Espionage
Percentage	22	20	13	12	10	8	6	5	2	2

Challenges and barriers to bridging the gap between cybersecurity and HR legal compliance

While bridging the gap between cybersecurity understanding and HR legal compliance is essential, organizations often face challenges and barriers in achieving this integration. One of the primary challenges is the lack of awareness and understanding of cybersecurity among HR professionals. HR departments traditionally focus on personnel management and compliance with labor laws, with limited exposure to cybersecurity principles. Overcoming this challenge requires organizations to invest in training and education programs that cater specifically to HR professionals, ensuring they have the necessary knowledge and skills to address cybersecurity risks. Another significant barrier is the complexity of privacy regulations and cybersecurity frameworks. Understanding the requirements imposed by regulations such as the GDPR or EU-GDPR can be challenging, especially for HR professionals who are not familiar with the intricacies of cybersecurity. Organizations must provide guidance and support to HR departments in interpreting and implementing these regulations, ensuring compliance without compromising security. Additionally, organizational silos and lack of communication between different departments can hinder collaboration in addressing cybersecurity and HR legal compliance. HR departments often operate independently, with limited interaction with cybersecurity teams or IT departments. Breaking down these silos requires organizations to foster a culture of collaboration and communication, encouraging cross-departmental cooperation and knowledge sharing.

Discussion

Creating a robust culture of cybersecurity within an organization is imperative to counter the escalating cyber threats. It underscores the shared responsibility of cybersecurity, stressing that every employee, not just the IT department, must actively participate in safeguarding against cyber threats. In this context, the HR department emerges as a valuable partner in promoting cyber hygiene and educating employees, given that a significant number of breaches result from human error. HR's role in safeguarding sensitive personal and financial data is particularly crucial, as this information is a prime target for cybercriminals. This analysis highlights the necessity of identifying and addressing various cyber threats, from phishing awareness to mitigating insider risks. Collaboration between HR and IT departments is key, as both must work in tandem to tackle cybersecurity challenges effectively, with HR professionals understanding the technical aspects of cybersecurity and IT professionals appreciating HR's data privacy concerns. It underscores the need for a comprehensive, organization-wide approach to cybersecurity that incorporates all employees and leverages HR's pivotal role in fostering a culture of cyber awareness while addressing both external and internal cyber threats.

Recommendations

The HR department can contribute to cybersecurity efforts within an organization. Cybersecurity is a critical concern in the modern business landscape, and involving HR in these efforts can be an asset.

- ➢ *Developing Security Policies and Guidelines*: HR can collaborate with the IT department to create and disseminate security policies and guidelines. These documents should outline best practices, acceptable use of technology, and expectations for maintaining security.
- ➢ *Cybersecurity Training*: Providing cybersecurity training to employees is crucial. This training should cover a range of topics, including email security, recognizing phishing attempts, and secure data handling. Regularly scheduled training and updates are essential as cybersecurity threats evolve over time.
- ➢ *Sensitive Data* Handling: HR plays a significant role in ensuring that new hires don't bring sensitive or confidential information from their previous employers. It's important to have a clear process in place to address this issue.
- ➢ *Managing Departing Employees*: When employees leave the company, HR should work closely with IT to

ensure all their access to systems and data is promptly revoked. Disgruntled former employees can pose a substantial cybersecurity risk.

- *Enforcing Security Protocols*: HR can emphasize the importance of adhering to security protocols and policies. They should also work with management to implement disciplinary consequences for employees who fail to comply with security measures. This can serve as a deterrent to potential security breaches.

6. *Background Checks*: Conduct thorough background checks on potential hires to identify any potential cybersecurity risks, such as past criminal activities related to cybercrimes.
7. *Incident Response Planning*: Collaborate with IT and management to develop an incident response plan that outlines the steps to take in the event of a cybersecurity breach. HR can have a role in ensuring employees are aware of and trained in these procedures.
8. *Security Awareness Programs*: Implement ongoing security awareness programs that keep employees informed about current cybersecurity threats and best practices.
9. *Vendor and Third-Party Security*: HR can also play a role in ensuring that vendors and third-party service providers meet cybersecurity standards, as their actions can also impact an organization's security.

HR's involvement in cybersecurity is essential to creating a strong security culture within the organization. By taking the steps you've mentioned and expanding their involvement in security-related activities, HR can help protect the organization from cyber threats and breaches [20].

Conclusion: *The future of cybersecurity understanding and HR legal compliance*

As the threat landscape continues to evolve, organizations must bridge the gap between cybersecurity understanding and HR legal compliance to protect sensitive employee data and ensure legal compliance. By investing in training and education programs, implementing cybersecurity policies and procedures, and fostering collaboration between HR and cybersecurity teams, organizations can create a more secure and compliant environment. The future of cybersecurity understanding and HR legal compliance lies in the integration of these two critical areas. Organizations that recognize the importance of this relationship will be better equipped to mitigate cybersecurity risks, comply with privacy regulations, and protect their employees' data. By prioritizing cybersecurity within HR departments, organizations can build a strong defense against cyber threats and safeguard their most asset their workforce [21]. Bridging the gap between cybersecurity understanding and HR legal compliance is not a one-time effort, but an ongoing commitment. As technology evolves and cyber threats become more sophisticated, organizations must continually adapt their strategies and practices. By embracing a proactive approach to cybersecurity and nurturing collaboration between HR and cybersecurity teams, organizations can establish a robust foundation for a secure and compliant future.

References

[1] Kumah, Peace & Yaokumah, Winfred & Buabeng-Andoh, Charles. (2018). Identifying HRM Practices for Improving Information Security Performance: An Importance-Performance Map Analysis. International Journal of Human Capital and Information Technology Professionals. 9. 10.4018/IJHCITP.2018100102.

[2] Nik Nordiana, Nik Ab Rahman & Widyarto, Setyawan. (2013). Information Security: Human Resources Management and Information Security Incident Management.

[3] Choi, Youngkeun. (2017). Human Resource Management and Security Policy Compliance. International Journal of Human Capital and Information Technology Professionals (IJHCITP). 8. 68-81. 10.4018/ijhcitp.2017070105.

[4] Ertan, Amy & Crossland, Georgia & Heath, Claude & Denny, David & Jensen, Rikke. (2020). Cyber Security Behaviour In Organisations.

[5] Guo, Yonggui & Cao, Lina & Gao, Xiao & Lv, Xuming. (2019). Understanding of the common methods in e-HRM data security. Journal of Physics: Conference Series. 1237. 022010. 10.1088/1742-6596/1237/2/022010.

[6] Zafar, Humayun & Stone, Dianna. (2021). Privacy, Security, and Legal Issues for HRIS.

[7] Ringim, Kabiru & Yusuf, Abdulmalik & Shuaibu, Halima. (2017). Effects of Human Resource Management Practices on Cyber loafing at Work. Yar'adua University Journal of Sociology (YUJOSO). 1. 279- 293.

[8] Zafar, Humayun. (2013). Human Resource Information Systems: Information Security Concerns for Organizations. Human Resource Management Review. 23. 105– 113. 10.1016/j.hrmr.2012.06.010.

[9] Michaelides, Nadine. (2021). Remote Working and Cyber Security Literature Review.

[10] Alshaikh, Moneer & Maynard, Sean & Ahmad, Atif & Chang, Shanton. (2018). An Exploratory Study of Current Information Security Training and Awareness Practices in Organizations.

[11] 10.24251/HICSS.2018.635.

[12] Vlachos, Ilias. (2008). The effect of human resource practices on organizational performance: Evidence from Greece. The International Journal of Human Resource Management. 19. 74-97. 10.1080/09585190701763933.

[13] Jabrayilova, Zarifa. (2015). PROBLEMS OF PROTECTION OF PERSONAL DATA IN HUMAN RESOURCE

[14] MANAGEMENT SYSTEMS. Problems of Information Society. 06. 22-28. 10.25045/jpis.v06.i2.03.

[15] Ahmadi H, Nilashi M, Shahmoradi L, Ibrahim O (2017) Hospital information system adoption: expert perspectives on an adoption framework for Malaysian public hospitals. Comput Hum Behav 67:161–189

[16] Ainin S, Parveen F, Moghavvemi S, Jaafar NI, Mohd Shuib NL (2015) Factors influencing the use of social media by SMEs and its performance outcomes. Ind Manag Data Syst 115(3):570588

[17] Cegielski CG, Bourrie MD, Hazen BT (2013) Evaluating adoption of emerging IT for corporate IT strategy: developing a model using a qualitative method. Inf Syst Manag 30(3):235–249

[18] Elia S, Massini S, Narula R (2019) Disintegration, modularity and entry mode choice: mirroring technical and organizational architectures in business functions offshoring. J Bus Res 103:417–431

[19] Izuagbe R, Ibrahim NA, Ogiamien LO, Olawoyin OR, Nwokeoma NM, Ilo PI, Osayande O (2019) Effect of perceived ease of use on librarians' e-skills: basis for library technology acceptance intention. Libr Inf Sci Res 41(3):100969

[20] Kraemer S, Carayon P, Clem J (2009) Human and organizational factors in computer and information security: pathways to vulnerabilities. Comput Secur 28(7):509–520

[21] Li L, He W, Xu L, Ash I, Anwar M, Yuan X (2019) Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. Int J Inf Manag 45:13–24