WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Study on Information Security in Human Resource Management

[1]Kanishka J, [2]Mr. Manoj Kumar, MBE, MBA

[1]MBA student, Jerusalem College of Engineering, Chennai
[2]Professor MBA, Jerusalem College of Engineering, Chennai
DOI: https://doi.org/10.55248/gengpi.5.0324.0919

ABSTRACT:

This research aimed to evaluate Information Security in Human Resource Management. A tailored survey questionnaire was distributed among a sample of participants from the organization to gather the requisite data. The collected data underwent analysis utilizing the SPSS V27 software. The study centered on the Information Security in Human Resource Management is Limited as both the study population and sampling unit. Findings indicated a positive Information Security in Human Resource Management, correlating with high levels of employee within the company. The study emphasizes the significance of Information Security in Human Resource Management. Moreover, it suggests further exploration into the impact across diverse sectors for future research.

Keywords Information Security, Descriptive analytical approach, Organizational research.

Introduction:

Information system means to consider available countermeasures or controls stimulated through uncovered vulnerabilities and identify an area where more work is needed. The purpose of data security is to make sure business continuity and scale back business injury by preventing and minimizing the impact of security incidents.

Confidentiality: Confidentiality refers to protecting sensitive information from unauthorized access or disclosure. This involves keeping confidential data secure and accessible only to those who are authorized to access it.

Authentication: Authentication is a crucial aspect of the principle of Information Security and is used to verify the identity of individuals or systems attempting to access sensitive information or systems. It is a process of verifying that a person or system is who or what it claims to be. Authentication is a critical component of Confidentiality and Availability as it helps prevent unauthorized access to sensitive information and systems.

Non-Repudiation: Non-repudiation is a principle of Information Security that refers to the ability to prove that an action or transaction took place and that it was performed by a specific individual or system. The term “non-repudiation” implies that an action or transaction cannot be denied by the individual or system that performed it.

Integrity: Integrity refers to the accuracy and completeness of information and the prevention of unauthorized or accidental modification of data. This ensures that data is not tampered with and remains trustworthy.\

HR professionals are actively embracing new technology

Technology is rapidly changing our world and your HR department is no exception. It is projected that technology would be more actively integrated into everyday HR functions. More and more companies are increasing their spend on HR tech year on year.But this rapid adoption of technology also increases the risk of cyber theft and cyber attacks. This enhances the need for cybersecurity for HR professionals. They need to balance technology with security, as they are more or less responsible for safeguarding all the technology-related activities at the workplace.The first step to cybersecurity starts with deploying regular software updates to fix the vulnerabilities in the security framework of the online network. A regular software update will keep the malware and hackers at bay and will help you safeguard your employee data.Also, HR professionals should create a good balance when providing access to sensitive software programs. They must make sure that they know who is granted access to the network and why. Plus, they need to regularly monitor the activities of employees on the secured network.A perfect ***Information Security*** system will help them maintain and monitor the online system and help protect it from any kind of cyber attacks from hackers. These vulnerabilities in your system, if they go unresolved or unpatched, your business and your online network will be susceptible to breaches and cyber attacks.

HR professionals safeguard personal data People in HR need to first understand that they have access to the perhaps the most sensitive information of the organization, which mainly includes employee personal information, such as their bank details, home address, personal identification details, contact number and date of birth, among others. This sensitive information is a gold mine of information for hackers.If this sensitive data or information is not

well protected with a secure network, then the information becomes highly susceptible to theft and attacks by hackers. Not just that you end up jeopardizing the security system of the entire network.HR cybersecurity will protect your sensitive data against any kind of cyberattacks. The professionals should have a detailed understanding of securing employee data from hackers. The sensitive information about the company payroll and company documents are like hot cakes for hackers.

They try to hack into these systems regularly. Most HR professionals are unaware of such a kind of looming theft. Understanding cybersecurity allows them to efficiently manage the systems and increase their awareness about cyber theft, which allows them to take a more responsible approach towards cybersecurity. To effectively implement HR cybersecurity, the company must conduct audits of the security systems at regular intervals and assess the potential threat to any of the sensitive information.

Literature review:

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. Nik Nordiana, Nik Ab Rahman & Widyarto, Setyawan. (2013). Information Security: Human Resources Management and Information Security Incident Management. 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.Ertan, Amy & Crossland, Georgia & Heath, Claude & Denny, David & Jensen, Rikke. (2020). Cyber Security Behaviour In Organisations.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. Zafar, Humayun & Stone, Dianna. (2021). Privacy, Security, and Legal Issues for HRIS. 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. 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.Michaelides, Nadine. (2021). Remote Working and Cyber Security Literature Review.Alshaikh, Moneer & Maynard, Sean & Ahmad, Atif & Chang, Shanton. (2018). An Exploratory Study of Current Information Security Training and Awareness Practices in Organizations. 10.24251/HICSS.2018.635.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. Jabrayilova, Zarifa. (2015). PROBLEMS OF PROTECTION OF PERSONAL DATA IN HUMAN RESOURCE MANAGEMENT SYSTEMS. Problems of Information Society.

Methodology:

This study combines both primary and secondary data sources. Primary data were collected through a well-structured questionnaire, employing a simple random sampling method to select 75 respondents. Secondary data were gathered from various reference materials, including books, journals, research articles, magazines, and websites. The research is classified under a descriptive research design, which focuses on describing the characteristics or behaviors of a phenomenon without manipulation or control. Descriptive research aims to provide an accurate representation of the subject under investigation and is commonly used to address questions such as "what," "who," "where," "when," or "how" about a specific topic.

Objectives:

- To study how the research is designed to comprehensively investigate on how Information security in Human Resource Management
- To study about shedding light on various dimensions associated with Information security in Human Resource Management
- Further, the findings of the study will be useful for future research to use it as a reference and secondary data.

Data Analysis and Interpretation

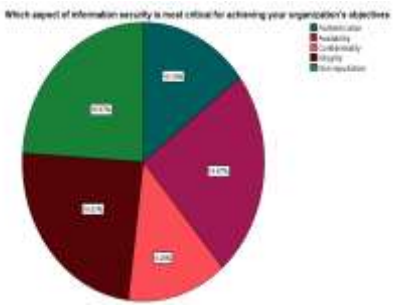
Percentage analysis

Percentage analysis **Which aspect of information security is most critical for achieving your organization's objectives**

TABLE 1

Which aspect of information security is most critical for achieving your organization's objectives

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Authentication	11	10.2	10.2	40.7
	Availability	18	16.7	16.7	57.4
	Confidentiality	10	9.3	9.3	66.7
	Integrity	18	16.7	16.7	83.3
	Non-repudiation	18	16.7	16.7	100.0
	Total	108	100.0	100.0	



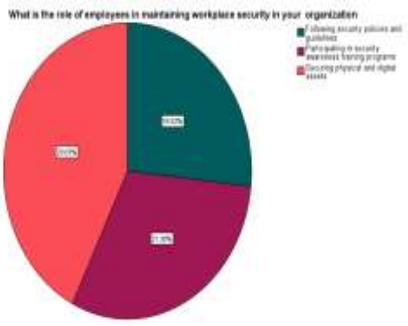
INFERENCE

According to the survey, out of 75 respondents,10.00% were Authentication, 18.30% Availability , and 9.11% Confidentiality, and 16.11% Integrity , 16.00% Non-repudiation

Percentage analysis What is the role of employees in maintaining workplace security in your organization

TABLE 2

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid					
	Following security policies and guidelines	20	18.5	18.5	49.1
	Participating in security awareness training programs	23	21.3	21.3	70.4
	Securing physical and digital assets	32	29.6	29.6	100.0
	Total	108	100.0	100.0	

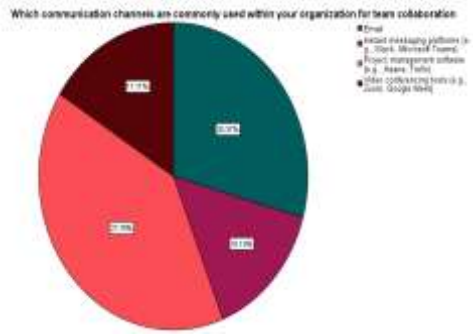


INFERENCE- According to the survey, out of 75 respondents,29.52% Securing physical and digital assets, 21.30% Participating in security awareness training programs, 18.52% Following security policies and guidelines

Percentage analysis of Which communication channels are commonly used within your organization for team collabora**tion**

TABLE 3

	Frequency	Percent	Valid Percent	Cumulative Percent
Email	22	20.4	20.4	50.9
Instant messaging platforms	11	10.2	10.2	61.1
Project management	30	27.8	27.8	88.9
Video conferencing tools	12	11.1	11.1	100.0
Total	108	100.0	100.0	

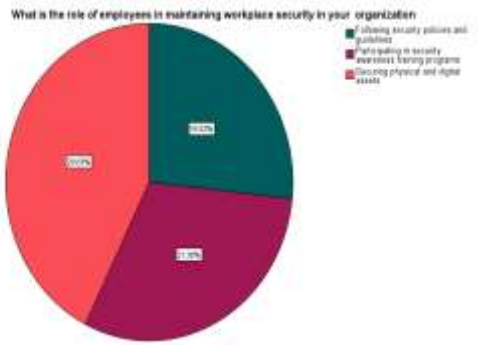


INFERENCE- According to the survey, out of 75 respondents 20.57% Email , 10.44% istant messaging platforms 27.67% Project management software, 11.11 Video conferencing tools (e.g., Zoom, Google Meet)

Percentage analysis for What is the role of employees in maintaining workplace security in your organization

TABLE 4

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid					
	Following security policies and guidelines	20	18.5	18.5	49.1
	Participating in security awareness training programs	23	21.3	21.3	70.4
	Securing physical and digital assets	32	29.6	29.6	100.0
	Total	108	100.0	100.0	



INFERENCE According to the survey, out of 75 respondents,29.52% Securing physical and digital assets, 21.30% Participating in security awareness training programs, 18.52% Following security policies and guidelines

CORRELATION ANALYSIS

To find the difference between communication channels are commonly used within your organization for team collaboration and How do you handle sensitive information and discussions during team communication in your organization

H0(null hypothesis): between communication channels are commonly used within your organization for team collaboration and How do you handle sensitive information and discussions during team communication in your organization

Hence H0 is rejected and H1 is accepted Therefore, There is a significance relationship between Which communication channels are commonly used within your organization for team collaboration and the How do you handle sensitive information and discussions during team communication in your organization

Correlations

		Which communication channels are commonly used within your organization for team collaboration	How do you handle sensitive information and discussions during team communication in your organization ?
Which communication channels are commonly used within your organization for team collaboration	Pearson Correlation	1	-486**
	Sig. (1-tailed)		.000
	N	53	53
How do you handle sensitive information and discussions during team communication in your organization ?	Pearson Correlation	-486	1
	Sig. (1-tailed)	.	
	N	53	53

Inference:

The calculated significant value 0.000 is lesser than the significant value 0.01 (0.000)

Hence H0 is rejected and H1 is accepted

Therefore, There is a significant relationship between Which communication channels are commonly used within your organization for team collaboration and the How do you handle sensitive information and discussions during team communication in your organization

REGRESSION

To find out the association between on how information security contribute to achieving in your organizational goals

Ho: There is no significance difference between on how information security contribute to achieving in your organizational goals

H1: There is a significance difference between How does information security align with the overall strategic objectives of your organization

Coefficients						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.797	.500		5.595	.000
	How does information security contribute to achieving in your organizational goals?	.128	.180	.084	.710	.480
	How does information security align with the overall strategic objectives of your organization	-.015	.165	-.011	-.092	.927
a. Dependent Variable: Which aspect of information security is most critical for achieving your organization's objectives						

Inference:

From the above table, we find that the significant value is 0.000, which is less than table value 0.05, so the Null hypothesis is rejected and Alternative hypothesis is accepted.

Therefore, there is a significance association between the number of dependents and to what extent do personal obligations affects ability to maintain a healthy work-life balance.

REGRESSION ANALYSIS

To find out the relationship between effectiveness of existing work-life balance policies and practices are implemented and enforced within the organization and perception of company culture.

Ho: There is no significant relationship between effectiveness of existing work-life balance policies and practices are implemented and enforced within the organization and perception of company culture.

H1: There is a significant relationship between effectiveness of existing work-life balance policies and practices are implemented and enforced within the organization and perception of company culture.

Coefficients [a]						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.728	.071		10.208	.000
	What is your perception of the company culture regarding work-life balance?	.373	.040	.669	9.356	.000

Inference:

From the above table, we find that the significant value is 0.480, which is greater than table value 0.05, so the Null hypothesis is accepted and Alternative hypothesis is rejected.Therefore, no significance difference between the overall satisfaction and the attention of the online advertisement.

Results

According to the survey, out of 75 respondents, 36.11% were male and 33.33% were female. And 10% respondents were respond According to the survey, out of 75 respondents, 46.00% were HR INTERNS and 23.15% were HR EXICUTIVES According to the survey, out of 75 respondents, 55.00% were Post graduates and 9.6% were Under Graduates and 2.78 were PhD holders According to the survey, out of 75 respondents,20.00% were ensuring compliance with regulations and standards , 21.30% Minimizing the risk of cyber threats and attacks , and 11.11% were protecting sensitive data from

unauthorized access , and 11.11% were safeguarding and integrity and availability of the systems and dataAccording to the survey, out of 75 respondents,10.00% were Authentication, 18.30% Availability , and 9.11% Confidentiality, and 16.11% Integrity , 16.00% Non-repudiationAccording to the survey, out of 75 respondents,14.81% were Ensuring business continuity and resilience, 13.89% Enhancing customer trust and loyalty , and 18.52% Protecting intellectual property and trade secrets According to the survey, out of 75 respondents,19.81% By enabling innovation and growth, 19.89% By ensuring regulatory compliance and avoiding penalties, and 12.52% By fostering a culture of security and trust, 18.52 By maintaining a competitive advantage in the market.According to the survey, out of 75 respondents,9.26%Being cautious of phishing attempts and suspicious emails, 15.74 Encrypting sensitive data before transmitting or storing it, 23.15% Following data handling procedures outlined in security policies , 21.30% Using strong passwords and authentication methodsAccording to the survey, out of 75 respondents 30% Others , 19.44% Mandatory additional security training, 16.67% Suspension or termination of employment, 16.67 Verbal warnings and counseling, 16.67% Written warnings and performance improvement plansAccording to the survey, out of 75 respondents , 15.74 Conducting regular team meetings and check-ins to discuss progress and address issues, 19.44 %Establishing clear communication protocols and channels for different types of messages ,30.37 % Setting expectations for response times and availability during working hours 13.50% Using collaborative tools that facilitate real-time editing and feedback on documents According to the survey, out of 75 respondents , 12% Conducting regular testing and monitoring of communication system for reliability and performance, 20.37 Ensuring compatibility with various devices and operating systems used by team members , 16.67 % Having backup communication channels in place in case of system failures or outages , 19.44 % Providing technical support and assistance to troubleshoot any issues with communication toolsThe calculated significant value 0.000 is lesser than the significant value 0.01 (0.000)Hence H0 is rejected and H1 is accepted , Therefore, There is a significance relationship between Which communication channels are commonly used within your organization for team collaboration and the How do you handle sensitive information and discussions during team communication in your organization we find that the significant value is 0.480, which is greater than table value 0.05, so the Null hypothesis is accepted and Alternative hypothesis is rejected. Therefore, no significant difference between the overall satisfaction and the attention of the online advertisement

Conclusion

The study, highlights significant trends, patterns, or insights discovered through data analysis. Emphasize any notable strengths or weaknesses identified in current information security practices within the human resource management context.

Highlight how improving information security practices can enhance data protection, mitigate risks of breaches or unauthorized access, and foster a culture of security awareness within the workforce.

References:

1. A Study on Information Security in Human Resourse – by Nik Nordiana Binti N Ab Rahman- Research gate.
2. Information Security Management- Jerry Bature Ansen