Journal of Positive School Psychology http://journalppw.com
2022, Vol. 6, No. 2, 4495 – 4501

A STUDY ON ROLE OF HUMAN RESOURCES IN CYBER SECURITY IN INDIA – With Special Reference to Cyber Risk Management

[1]Dr. R. Menaka

[1]Assistant Professor, Department of Management Studies (DDE), Madurai Kamaraj University Madurai-625021

Abstract

The human resources (HR) work has become basic to organizational cyber hazard management lately. Alongside data security/data innovation (InfoSec/IT), HR is progressively called upon to help decide and uphold representative information authorizations, prepare and implement cyber security arrangements and methods, and help react to cyber occasions including workers. HR's expanded involvement is because of a union of variables, including a more dynamic administrative environment, the inescapable utilization of innovation and gadgets in representatives' work, and acknowledgment of the significance of a solid organizational cyber security culture. Workers' information and security rehearses are basic determinants of an organization's general cyber security. Close to 66% (62%) of leaders say the best danger to their organization's cyber security is workers' inability to consent to information security rules, not programmers or sellers, as per Mercer's 2020 Global Talent Trends Study. However HR isn't ordinarily an essential proprietor or driver of cyber hazard management, as found in Marsh and Microsoft's 2019 Global Cyber Risk Perception Survey. The incredible greater part (88%) of organizations keep on appointing cyber hazard as a matter of first importance to InfoSec/IT, trailed by the C-suite, hazard management, legitimate, and finance. These necessities to change a solid organization between InfoSec/IT and HR is fundamental for managing information and innovation hazard, especially in a remote-working environment. Underneath we investigate four key regions where the advancing administrative and cyber hazard scenes are changing HR's job. Hence, the current study has been done to highlight the role of human resources in cyber security in India.

Keywords: Information Evidences, Disciplinary Ramifications, Security Policies, Preventative Strategy, Cyber Risk, Cyber Attacks and Protocol Network.

INTRODUCTION

HR is typically the first and last resource for representatives, and accordingly assumes a significant part in making and keeping a hearty cyber security culture. In spite of the fact that IT customarily made cyber security instructional courses, HR's involvement has expanded as the significance of such preparing for workers has become better perceived. Data gave to new workers regarding how to rehearse great cyber security cleanliness in their every day undertakings, can extraordinarily influence their certainty if or when defied by a situation expecting them to relieve a cyber hazard. Preparing ought to incorporate direction for perceiving and dealing with normal situations, for example, phishing and secret phrase security. It ought to likewise incorporate how to deal with the organization's computerized change and implementation of new innovation, just as best practices for bring-your-own-gadget, remote access, business coherence, occurrence reaction and recuperation, and utilization of gadgets.

The COVID-19 environment makes preparing and strategy consistence significantly more basic, considering that work-from-home cyber security conventions and practices may not be pretty much as powerful as should be expected

office conditions. A solid cyber security culture should likewise incorporate ramifications for resistant conduct. HR and IT need to team up to impart the consequences for not after best practice security strategies, or not finishing preparing for which more workers are being punished in their performance surveys and even remuneration. A powerful cyber security culture begins from the highest point of the organization and includes ceaseless correspondence and preparing for pioneers across every single key capacity. Table-top activities recreated cyber occasions that test an organization's reaction are profoundly valuable for adjusting the activities and needs of IT, PR, hazard management, C-suite, board individuals, and lawful/consistence.

Genuine venture cyber hazard management programs remember HR for these reaction testing works out. Other than HR's significant job in cyber hazard management arranging, its incorporation in occasion reaction arranging can help adjust the considered treatment of representatives with relevant employment guidelines and laws and assist with alleviating the danger of expected case.

OBJECTIVES OF THE STUDY

The study aimed with following objectives:

1. To know the cyber security in the digital era of human resources.

2. To summate the different secondary sources related to the study.

REVIEWS OF RELATED LITERATURE

Ertan et al. (2020) have done a research and it explores the scholastic and strategy writing with regards to regular cyber security in organisations. In this manner, it recognizes four social sets that impacts how individuals practice cyber security. These are consistence with security strategy, intergroup coordination and correspondence, phishing/email conduct, and secret phrase conduct. Notwithstanding, note that these are not thorough and they don't exist in seclusion. Furthermore, the audit investigates the thought of safety culture as an all-encompassing topic that covers and casings the four social sets. The point of this survey is subsequently to give a rundown of the current writing in the space of ordinary cyber security inside the sociologies, with a specific spotlight on organisational settings. In doing as such, it fosters a progression of ideas for future examination headings dependent on existing holes in the writing. The audit likewise incorporates a hypothetical focal point that will help the comprehension of existing investigations and more extensive written works. Where conceivable, the survey makes recommendations for organisations corresponding to ordinary cyber security.

Kumah et al. (2018) have done a study and it was centered on distinguishing key human resource management (HRM) rehearses vital for further developing data security performance according to the viewpoint of IT experts. The Importance-Performance Map Analysis (IPMA) by means of SmartPLS 3.0 was utilized and 232 examples were gathered from data innovation (IT) experts in 43 organizations. The investigation distinguished data security preparing, historical verifications and checking as vital HRM rehearses that could work on the performance of organizational data security. Specifically, the review tracked down preparing on cell phones security and malware; individual verifications and checking of potential, current and previous representatives as of high significance however with low performance. Accordingly, these key regions should be improved with first concern. On the other hand, the review tracked down responsibility and representative relations as being excessively underlined by the organisations. The discoveries raised some valuable ramifications and data for HR and IT pioneers to consider in future data security system.

Choi, Youngkeun. (2017) have summarized an investigation as given the administrative requirements forced on organizations inside various businesses, research in the space of worker consistence with organizational security and protection guidelines stays fundamental and profoundly attractive. Consequently, the goal of this review gives a one of a kind structure to understanding the impact of HRM rehearses on individual security strategy consistence results. The unit of investigation for this examination project is the singular representative of a bank organization. With the review of 257 bank representatives, a parts based way to deal with primary condition demonstrating was taken. The

consequences of this review show that developmental-situated examination, remotely or inside impartial award, particular staffing and preparing for vocation development are decidedly connected with workers' conduct expectation to go along security strategy through their full of feeling commitment.

CYBER SECURITY IN THE DIGITAL ERA OF HUMAN RESOURCES

Cyber security in this computerized age is turning into an organizational concern. Many individuals don't imagine that HR experts, for example, have nothing to stress over when data spills, information hacks, and personality robberies occur. Notwithstanding, every worker needs to rehearse fundamental cyber cleanliness for an organization to be protected. HR experts handle a ton of delicate business information. This incorporates worker individual data, compensation subtleties, and so forth, which can cause enormous harm whenever spilled. Along these lines, HR experts are in an amazing situation to forestall cyber dangers. This article investigates the job of HR in an organization's cyber security. The following are a couple of ongoing patterns in HR experts can do:

Identify an Organization's Risk Exposure

The initial step to forestalling dangers is remembering them. An organization's HR can decide its danger openness by consistently leading a danger assessment. Standard assessments assist with building up what unsafe worker practices can open an organization to information breaks or different dangers. For example, a danger assessment by HR can assist an organization with finding an unstable workstation. It can likewise uncover whether workers have lost their ID cards. These are representative blunders that can give cybercriminals touchy data or uncensored admittance to an organization's organization.

Additionally, hazard assessments assist organizations with redoing their preparation modules. It tends to be trying to give the right sort of representative preparing on the off chance that you don't have the foggiest idea what dangers your organization could be helpless against, making hazard assessments considerably more imperative.

Employee Data Controls and Access

There is an assortment of ways of ensuring touchy information. One of them is setting up various access controls to this data. A decent information management methodology needs access controls to guarantee that main a particular arrangement of individuals can see or utilize the information put away on an organization's organization. The HR department can help a business set up and implement access controls. HR can characterize the information that a representative requirements to utilize even prior to recruiting or onboarding them. They likewise need to guarantee that the worker doesn't approach this data toward the finish of their agreement.

Fortunately, there are some IP pivoting private intermediaries and other advanced arrangements that can assist them with doing this. HR can utilize intermediaries to keep access from workers once they end their agreements. Intermediaries can empower HR to keep away from insider risks arranged by previous workers who have some type of admittance to organization organizations. It has become hard to work without tech arrangements in each business viewpoint. Intermediaries are a portion of the tech arrangements assisting organizations with moving forward and manage cyber dangers. They make getting touchy information simpler and increment the odds of a business' security technique succeeding.

Help in Security Policy Making

Security strategy making is vital for organizations. Each department, including HR, plays a part in making and implementing organizational security approaches. This guarantees that the firm, its customers, and the labor force are consistently protected from various dangers. The job of HR in arrangement making and implementation begins during recruitment. They need to do consensual pre-employment historical verifications to know their planned recruits more. They additionally need to give representatives with a set of accepted rules and sign it prior to employing them.

Additionally, HR needs to scramble all representative records and have arrangements on how workers can get to them. HR must work with an association's management when representatives disregard rules. They should

participate in the examination and furthermore assist with squeezing charges against offenders.

Promote a Cyber security Culture

Actually, advancing a cyber security culture in an organization is everybody's job. HR is perhaps the most basic player with regards to making and sustaining organization culture. This is on the grounds that it is the first and last representative contact point in each organization. The HR business needs to show representatives why the organization's cyber security matters. It likewise needs to characterize the representatives' job in guaranteeing the's organization is protected early enough. This will assist with decreasing disregard as it will bring a feeling of obligation.

Recently added team members likewise need to see the cyber security culture whenever they first communicate with the organization through HR. This is on the grounds that as of late on boarded workers can be the most vulnerable connection in an organization. Making an attitude in them that the danger is genuine and their everyday activities sway that hazard is fundamental. A hearty cyber security culture ought to consistently exist inside a business. It needs to begin from the top management and stream down to an association's workers. The HR and other departments need to cooperate to guarantee that each new worker comprehends the way of life and fits in well.

Educate Employees on Cyber security

For data security to be powerful there should be a consistent preparing process. Each organization needs to prepare its representatives on data security consistently. This guarantees that workers perceive cyber security as a standard business practice and adhere to the organization's prescribed procedures. The HR department plays a huge part to play in worker data security preparing. They need to incorporate security bits of preparing into fresh recruit directions. This incorporates stressing the dangers that the firm is powerless against and what representative practices can assist with keeping them from occurring.

A strong security-mindfulness program can help a business support its security. Through preparing, representatives who have not gone over information breaks and hacking can respond suitably. These assist with forestalling risks, for example, phishing or radically diminish their danger. Each piece of preparing should push the arrangement that an association's cyber security is everybody's obligation. This makes it simple to implement approaches and even advance the security culture we mentioned above.

ANALYSIS PART OF THE STUDY

Table 1: *HR Needs about Cyber security in 2021*

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%

Source: Ponemon/IBM

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 %

Source: Ponemon/IBM

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

Source: CyberEdge Group 2021 Cyberthreat Defense Report

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

Source: Global Information Security Survey

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

Source: Global Information Security Survey

DISCUSSIONS AND RECOMMENDATIONS

With regards to making a culture of cyber security inside their organizations, one thing is clear: Changes should be made all through the helpful, in addition to the IT department. A characteristic accomplice in fostering a more grounded cyber security act is the human resources department. When 95% of breaks are a consequence of an organization's own labor force, HR experts should be engaged with making a culture of cyber security and assisting representatives with taking on great cyber cleanliness propensities. Organizations that don't find every one of the vital ways to secure their kin and organizations leave the entryways totally open to cyberattacks that could cost thousands in income, information and lost representative trust. The HRPA plunked down with George Finney, Chief Information Security Officer and CEO and author of Well Aware Security, to find out about how HR experts, close by IT, can assist with shielding their workers and organizations from vindictive programmers. While figuring innovation experiences made our lives dramatically difficulty free, it additionally has cleared way for a plenty of dangers as far as information robbery, security break and hacking. Cyber security infringement are damaging and can cause enormous misfortune for a business be it little or large. The most incredibly upsetting reality here is that almost half of the workers (the ones being laid-off or terminated) will more often than not take private corporate information in the wake of stopping. Additionally, reckless goofs from representative's characteristic to a gigantic piece of cyber security break at working environments. In this way, organizations should be cautious of the outer cyber dangers, yet additionally from the potential penetrates that can happen inside the organization from its own staff.

Given the way that an organization's own staff maneuvers a greater part of cyber-risks, human resources department alongside the IT group can assume an essential part in battling the battle against conceivable cyber security dangers. This

is the justification for why IT and HR need to collaborate. This is especially evident since the information that human resources staff manage is exceptionally inclined to security risks. HR data set regularly involves profoundly private and touchy data, for example, bank subtleties, birth dates, contact subtleties, PAN number, addresses to give some examples. This is the justification for why HR people need to have an exhaustive comprehension of how to protect such information from likely programmers and security risks. Before conceiving a deterrent technique, it is basic for the human resources experts to recognize potential cyber dangers. A colossal number of organizations today have progressed programming answers for check the dangers of outer cyber-risks like infection or malware. Phishing is one such illustration of outer cyber danger where the impersonator stunts representatives to outfit basic data, regularly through email. Programmers are even answered to copy work messages from a clearly reliable source, which the representatives open when at work. These messages can contain noxious infection or malware that the programmers can secretly use for getting to delicate information of the organization. Other than phishing, other normally detailed dangers imply reckless goofs from representatives like losing or messaging basic information to unknown sources/beneficiaries, logging from an uncertain web convention network when out of the working environment and cognizant noxious cyber-risks from previous representatives or current ones.

Recommendations

HR can assume a critical part in controling cyber security dangers. However the dangers are both dangerous and upsetting, HR experts can assume a vital part in battling against cyber-wrongdoing at work. Here's the way they can prevail with regards to doing that:

1. Human resources department can help the IT group in creating and engendering security arrangements and rules across the organization.

2. One of the best deceives is to prepare the whole HR staff on cyber security conventions. This becomes fundamental for recently enrolled representatives. The preparation should be a vital piece of the on-boarding process wherein the recently enrolled people are told about issues identified with utilizing and getting to delicate information close by furnishing them with essential cyber security preparing. The preparation no matter what ought to incorporate email security and methods of distinguishing possible malevolent substance.

3. Human resource work force should ensure that recently selected representatives don't have any touchy or secret information from their ex-manager.

4. It is prudent to close every one of the internet based records of previous representatives when they leave the organization. This is on the grounds that the greater part of the cyber-risks detailed happen when a representative leaves the organization.

5. HR groups ought to likewise weight on the disciplinary consequences for representatives, who neglect to submit to the security conventions.

CONCLUSION

While the cyber security danger can never be completely killed, in advance of mentioned data proves that the dangers can be controlled fundamentally through a successful and proactive human resource management methodology. Eventually, the greatest and tragic danger to an organization’s cyber security is that of its own kin. The objective is to be proactive rather than being responsive with regards to cyber security. Individuals are fragile and botches do will generally occur. All things considered, setting up brief HR, security strategies and conventions can alleviate such dangers by and large.

Those are a portion of the manners in which that HR can add to an organization's cyber security. In any case, this rundown isn't comprehensive as there are many more things that HR can do. For example, HR is additionally liable for observing telecommuters since they present greater security dangers to an organization. We have as of now mentioned fundamental jobs of HR, like approach making. HR needs to keep up with well-documented approaches and guarantee that each fresh recruit gets them. This incorporates methodology for detailing dangers, reacting to them effectively, and so on, to defend a firm and

its information. The rising danger of cybercrime has made security too basic to even consider neglecting. Also, it has made web-based security an entire organization's job and not just for data innovation security trained professionals. The experiences mentioned above can help HR experts contribute emphatically to a company's cyber security.

Reference

[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. 10.24251/HICSS.2018.635.

[11] 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.

[12] Jabrayilova, Zarifa. (2015). PROBLEMS OF PROTECTION OF PERSONAL DATA IN HUMAN RESOURCE MANAGEMENT SYSTEMS. Problems of Information Society. 06. 22-28. 10.25045/jpis.v06.i2.03.