Section: Research Paper

HR Dynamics in establishing cyber security measures in the Indian banks

SREEKAR G.S.G (Research Scholar)
kiransreekar@gmail.com
Prof. PADALA VISWANADHAM (Guide)

Department of Commerce and Management Studies, Andhra University, Visakhapatnam- 530003, Andhra Pradesh.

Abstract: Indian banks have been progressively digitizing their operations, cyber security in the banking industry has grown more challenging than ever. Sharing vital sensitive information with staff and customers in a safe manner is becoming a challenging procedure to prevent data theft or attacks from hackers and cyber criminals, especially in the banking sector. Most of the sensitive information is accessible by the HR departments of the banks, therefore, protecting the bank's as well as customers' information online from risks like malware, viral assaults, and hackers falls under the Human resources department's purview. With such a weighty duty on their shoulders, HR professionals need efficient and effective cyber security measures to safeguard the bank's software system. Cyber security for HR professionals is now more important than ever because the organization and its customers transmit so much information online. The heavy burden of establishing secure and cyber-safe measures falls on the HR department. The study elucidates why and how HR plays a vital role in establishing cyber security measures in the banks and what strategies, techniques, and patterns are encountered while implementing the process.

Keywords: HR Dynamics, Cyber security measures, Cyber-hygiene, Cyber-talent retention.

Introduction: The HR department is never an exception in the fast-changing technology. Technology is predicted to be more actively integrated into everyday HR functions. More and more companies are increasing their spending on strategic HR technological innovations each year. However, the rapid adoption of this technology also increases the risk of cyber theft and cyber-attacks. This increases the need for cyber security for HR professionals. They need to balance technology and security because they are more or less responsible for protecting all technology-related activities in the banks. The first step in cybersecurity begins with the provision of regular software updates to address vulnerabilities in the online network security framework. Regular software updates keep employees away from malware and hackers and protect banks' customers' data.

In addition, HR professionals need to balance when granting access to sensitive software programmes. The HR manager needs to know who is allowed access to the network and why. He should also regularly monitor employees' activity in a secure network. A perfect cyber security system helps maintain and monitor the online system and protect it from all kinds of cyber-attacks by hackers. If these vulnerabilities in the system are not fixed or patched, the whole transactions in the banking and online networks are vulnerable to security breaches and cyberattacks.

To analyse a recent example, several customers of HDFC Bank in Chennai, India were bewildered to discover that their bank accounts had been erroneously increased by millions on Sunday 29 May 2022. A technical error during a system upgrade increased the bank balance of 100 customers by thousands of rupees to 1.3 billion rupees. According to media reports, the incident was reported by

a few outlets in the city and a total of 1.3 billion rupees was transferred to customers' accounts. One of the customers claimed that his wife's account balance had dramatically increased by Rs 1.23 crore without credit and the surplus was gone by the evening. Even in such situations if the customer withdraws or transfers money to another account of his own, in such dramatic situations, as per the law, the bank should recover the loss but if anyone with an ingenious mind-set wants to misuse such opportunities by disappearing with the credited money to another country, then it becomes highly complicated to put the criminal behind the bars.

Literature review: 'Cyber Self-Defence' is a book of advice on how to avoid online predators, identity theft, and cyber-bullying. ALEXIS MOORE, the author of the book guides us with practical examples and real-life situations to keep us safe from those around us who may be using the internet to cause trouble. The author elucidates the 10 most common profiles of cyber-stalkers. Some of them are attention-seeking, jealous, manipulative, controlling, and narcissistic.

The author discusses the menacing behaviour of cyber stalkers in detail. Each chapter of the book includes a quiz to help the readers identify signs of this personality type to determine if they are potentially vulnerable. There are also tips for preventing or recovering from many kinds of cyber-crime. The techniques range from recovering data, monitoring online profiles, protecting social media information, regaining self-esteem and changing identities, etc.

'Digital Banking and Cyber Security' is a marvellous book covering various practical examples of data breaches resulting in high vulnerabilities. The author Dr. Sarika R Lohana throws light on different security issues to be resolved immediately. According to her, it may be man-made or even natural unintentional data exchanged online can be misused by anyone. A beginner in cybercrime also can cause a huge loss if the victim is not careful. Cyber-attacks are prevalent among individuals, businesses, government organizations, and particularly banks. The cyber-attacks can take the form of (a) phishing, (b) hacking, (c) scamming, (d) sniffing, (e) spoofing, and (f) denial of service attacks, etc. With the changing face of a fraudster, the Human resource department in the banks faces typical challenges daily.

Scope of the study: The study focuses on the various challenges faced by human resource managers in establishing cyber security standards in the banking sector and discusses the various ways in identifying the right cyber talent to match the current problems and suggests some possible recommendations while focussing on the strategies adopted by the HR department to create cyber security awareness in the customers.

Hypotheses:

- HR plays a more important role than the IT department in a bank in the establishment of better cyber security policies.
- The HR department plays a more decisive role than any other department in a bank in creating better cyber security hygiene/measures.
- The HR's cyber security awareness strengthens the banks with the best security policies.

Objectives of the study: The study specifically focusses on the following areas.

- The challenges encountered in finding cyber security experts with ultra-practical knowledge.
- Challenges faced in the retention of quality cyber talent.
- Extensive In-house Employee cyber security training & challenges.
- Continuous, comprehensive training, spreading awareness on customer cyber-education.

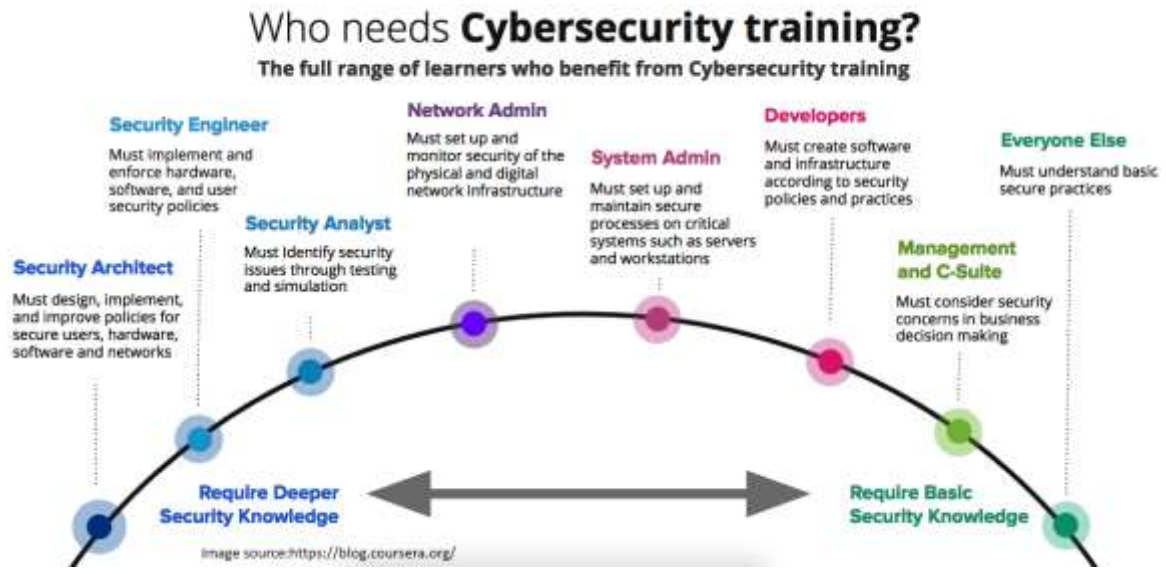
- Dealing with cyber-illiterate customers.
- Strategies in dealing with the customers' complacency towards cyber-hygiene.
- Efforts to bring the latest cyber-crimes into the purview of cyber laws.
- HR's role in finding out the best solutions to the current cyber security issues in the banks
- HR's needs in procuring enough budget for Cyber security in the banks
- Creating relevant policies
- HR Dept. Working parallel with the IT Dept.
- Empowering the employees with the right tools

The circumspective role of HR department:

Most of the banks' cyber-attacks are carried out by the attackers, who have clearly understood the lacunae in that particular bank's security system. The human resources department and the IT team can play a key role in fighting against possible cyber security threats. The IT and the HR departments need to work together because their coordination plays a vital role in the successful identification of checking/resolving the issues. Since human resources personnel deal with highly confidential and sensitive information, databases are particularly prone to security breaches. The HR professionals need to coordinate with the IT department while imparting the right training.

The image below depicts the range of learners who benefit from the cyber security training

Fig.1: The learners who need and benefit from cyber security training.



Threat identification:

Human resources specialists must identify potential cyber hazards before coming up with a protective approach. The modern banking industry uses sophisticated software to reduce the hazards of external cyber-attacks like viruses and malware. One such instance of an external cyber threat is phishing, in which the fraudster entices employees into providing crucial information, frequently by email. Even fake emails from an ostensibly reliable source that employees/customers open while at work have reportedly been sent by hackers. These emails may be infected with malware or viruses that hackers can employ to access the users' private information. In addition to phishing, other often reported dangers include thoughtless errors made by the banking staff such as losing or transmitting sensitive information to unidentified sources or recipients and logging from the wrong computer.

Challenges in finding the right cyber security experts:

One of the biggest challenges that has ever been faced by the HR department is finding the right cyber security supplier because of the problems in confiding in the very security provider as the whole banking is related to financial transactions, relying too much on any one single source extravagantly lands the whole banking in trouble. Finding the right talent is not easy as many cyber security professionals are just hired on the spot and have a huge demand in the market.

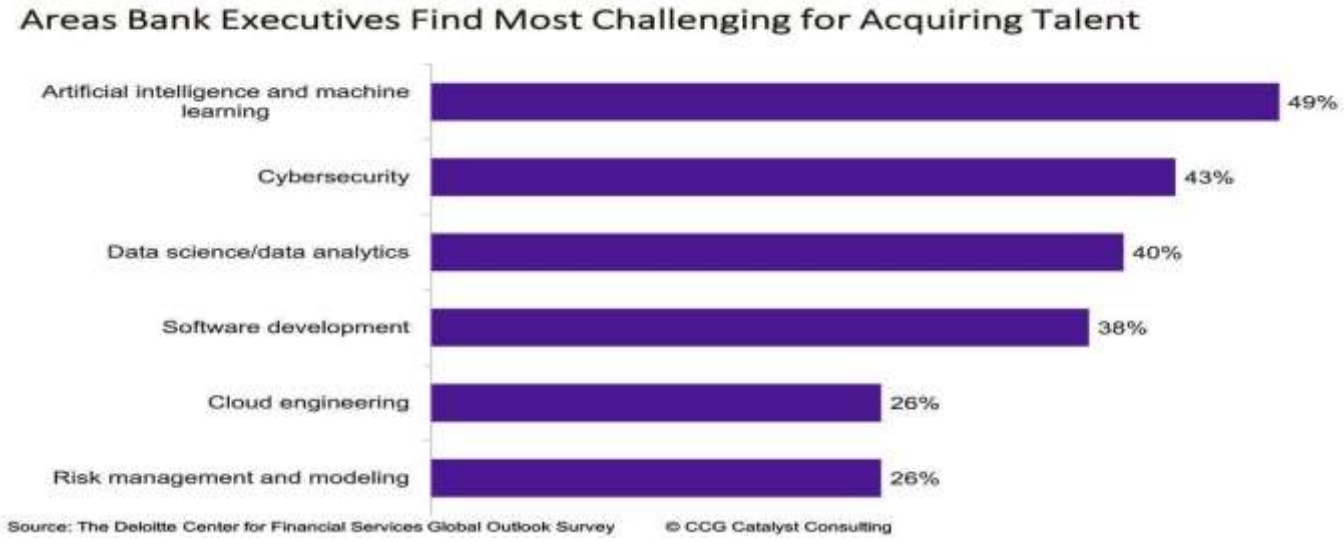
Retention of quality cyber talent:

As predicted three and a half million cyber security roles would go unfilled by 2023, and the number of qualified cyber security specialists is not increasing to match the demand. When hiring for cyber security positions, banks must contend with more than just a scarcity of qualified candidates. The difficulty of retaining cyber security expertise is new, and typical retention techniques frequently fail to resolve the issues. Retaining talent is difficult in the fast-paced and distinctive industry of cyber security. Many HR departments in the banks mistakenly believe that giving their employees adequate training makes them more likely to quit for higher-paying opportunities with rival organizations. The truth is that the training helps employees feel valued by the banks, which in turn encourages them to make investments in the banking sector business.

In-house Employee cyber security training & challenges:

Nearly all public spaces need to be secure. Security is a crucial component of many organizations, whether it's intended to protect customers, keep employees safe, or safeguard the area's assets. Security is of the highest concern to banks and credit unions. For banks and other financial organizations to be able to safeguard the money they are trusted with as well as the people who frequently visit the institution, physical and digital security are essential. Proper training is the greatest approach for any financial institution to keep things safe and secure.
Employees at banks fill a variety of positions, from IT to tellers to sales to marketing, and many of them work in a specific branch for many years, developing a particular manner of operating. Delivering training material that improves the bank's security posture while having a favorable effect on these long-term employees' behavior and having no negative effects on their productivity or morale is a problem.

Fig.2: The areas HR finds most challenging for acquiring talent



Continuous, comprehensive training, spreading awareness on customer cyber-education:

The very source of income in all businesses is the customer, but carelessness and complacency of the customers can be very expensive in the banking sector. Cyber-illiteracy proves fatal in the digitalized era of banking. For the last ten years every day, there have been numerous cyber-attacks because of the sheer ignorance and cyber-illiteracy, and negligent attitude of society.

A digitalized bank with a majority number of illiterate customers would generally become the first victim of such attacks. Lack of education and awareness costs a lot not only to the customers but also to the banks. The poor illiterate folk who have lost money trusting a third-party mobile call asking them to share an O.T.P. or sensitive information don't know even how they got cheated and continue to suffer forever. Knowingly if an O.T.P. is shared trusting a fraudster's call even no cyber law can protect the victims. The victims are looted for no fault of their own, become helpless and even some of the victims lose the entire money saved in the banks and even there were incidents when these victims committed suicide helplessly.

When a customer opens an account in the bank, the HR department can think of giving rigorous training to every customer before completing the account opening formalities irrespective whether the customer is educated or not. The customers can be given detailed instructions on how cyber-attacks happen and how to safeguard from them and in what way they can be aware of such issues. In the process of creating cyber awareness in the customers, each customer can be made to undergo a comprehensive test covering various aspects of cyber-attacks and strategies to better cyber security practices. This testing process has to be made mandatory for every customer before opening an account with the bank.

Recommendations:

Set up training and awareness workshops as necessary: The most effective thing the HR department can do is educate all its personnel on cybersecurity best practices. Employees must get training on matters involving accessing and using sensitive customers' data. Cyber security education and awareness seminars must be considered a crucial component of the on-boarding process for newly hired staff.

The fundamental security instruction must cover the following

- How to create awareness in the customers to select secure password combinations for the online account login and how to select appropriate security questions.
- How to protect the security and integrity of e-mail?
- How to recognise fraudulent activity and online frauds, etc.
- Secured O.T.P. sharing practices.

Build up holistic security competencies: Hackers don't just enter a bank's network blindly when they seek to break it. They conduct thorough research to develop sophisticated attack strategies by learning about network security, personnel, and weaknesses. Hackers typically utilize social media to choose a target and then bypass security measures**.** To locate a trigger event, such as dismissal, or even redundancy, the hackers may even develop a connection with the target customer. This would allow them to psychologically influence the target. This is precisely why the HR team must be alert at all times to detect such possibilities, intervene, and deter them. Regular check-ins and

mock drills will allow the HR department to identify weak links. For example, it is common for an organization

to send bogus emails posing as from well-known brands and requesting personal or confidential company information. Customers who open such emails and respond with details can be educated on email security. Many banks track and monitor their customers' browsing habits.

Creating practical and relevant policies: Security policies are essentially statements that outline the decision-makers' responsibilities for safeguarding a bank's critical physical and information systems. These policies are not intended to provide a technological solution to cyber threats, but rather to inform employees and customers of the intentions and conditions that will help to safeguard a bank's security controls.

One of the key functions of the HR department is to create procedures and protocols and to ensure that the employees are aware of the standards that have been established. This will assist banks in controlling the threat and reducing the overall damage. These policies must include not only the precautions to be taken to avoid a security breach, but also the immediate steps that can be taken in the event of a breach, which would include changing all employees' login credentials, informing employees and customers of a possible data leak, diagnosing the cause of the breach, and making changes to prevent it in the future.

Conclusion:

A proactive cyber security assessment/audit is advised in every phase and a comprehensive threat assessment using the spot risk-based approach is deemed to be one of the practical solutions to security issues, on the other hand, cyber security maturity assessment for all the employees should be made mandatory while bridging the lacunae in the whole security system, saves time and further loss. According to priorities, closing the gaps will be necessary to raise the actual degree of resilience to the desired levels. To achieve this, a roadmap must be identified and created to raise the efficiency to the desired levels.

Cyber risks interact with one another and change with time so the HR team has to make continual monitoring necessary to enable the desired response. Understanding the evolving nature of fraud and money laundering techniques is thus a crucial first step. Fraud risks are no longer isolated instances of loss brought on. Money laundering is no longer just transactions with fictitious identities. Hacking into a bank's network has made it possible to commit fraud, which has a ripple effect and a systemic consequence. It is vital to monitor and report on these changing patterns using an integrated lens.

Cyber threats are dynamic, the banks need to prioritize their efforts and invest in crucial cyber sectors to manage the threats and safeguard vital assets. The administration of the bank's security posture is suggested to make simple by Check Point's network security solutions, which also streamline and scale business operations. Concerning Gen V cyberattacks on the network, cloud, data center, IoT, and distant users, the ‘Quantum Network Security solution’ offers ultra-scalable defense.

Banks must ensure that cloud assets and data are secure and compliant with rules such as those from the European Banking Association (EBA) and the US Federal Financial Institutions Examination Council (FFIEC) as they migrate data and workloads to the cloud (EBA). Modern cloud deployments, however, are incredibly intricate, therefore, even when public cloud providers make

significant security investments, it is still the bank's HR's responsibility to ensure the organization's cyber security.

With the ever-brimming criminal mindset of the cyber criminals searching for technical lacunae and new malware scripts/codes being created, multiplied, and executed daily, the challenges of the HR department in establishing cyber security measures is never ending but with the ultra-practical approaches and dynamic strategies it is not impossible to outpace the cyber-criminals.

References:

[1]. Countering Cyber Threats to Financial Institutions: A Private and Public Partnership Approach to Critical Infrastructure Protection Book by David L Lowery and Pierre-Luc Pomerleau

[2]. Digital Banking and Cyber Security Book by Sarika R. Lohana

[3]. Cyber Security Issues and Current Trends: by Nitul Dutta, Nilesh Jadav, Sudeep Tanwar, Hiren Kumar Deva Sarma

[4]. Cybercrime Storytelling Blue Screen of Death by Donnie Skane

[5]. Countering Cyber Threats to Financial Institutions a Private and Public Partnership Approach to Critical Infrastructure Protection: Authors: Pierre-Luc Pomerleau, David L. Lowery: https://link.springer.com/book/10.1007/978-3-030-54054-8

[6]. The Role of Human Resources in Cyber security: Tom Glover President of Responsive Technology Partners:https://www.linkedin.com/pulse/role-human-resources-cyber security-tom-glover

[7]. The role of HR in managing cyber security issues in the banks: SREEKAR G.S.G Journal: Specialusis Ugdymas. https://www.sumc.lt/index.php/se/article/view/610

[8]. The importance of HR's role in cybersecurity: By Isabella Harford, Assistant Site Editor: https://www.techtarget.com/searchsecurity/feature/The importance-of-HRs-role-in-cyber security

[9]. The Role of HR in Managing Cybersecurity - Hacker Earth

[10]. Cybersecurity – an Important Aspect for HR Professionals HUMAN RESOURCE Shalini L https://www.betterplace.co.in/blog/importance-of- cybersecurity-for-hr-teams/

[11]. What Role does HR Play in Cyber Security? By Kathryn O'Connor: https://www.hrsource.org/maimis/ Members/Articles/2018/07/July_17/ What_Role_does_ HR_Play_in_Cyber_Security_.aspx

[12]. The Role of HR Mitigating Cyber Security Threats: https://www.netatwork.com/the-role-of-hr-mitigating-cyber security-threats/

[13]. Role of HR in Banking by David Ingram: https://bizfluent.com/info-7986688-role-hr-banking.html

[14]. Cyber security - is HR a target? Published in the month of January 26, 2022 by Kit Barker: https://www.myhrtoolkit.com/blog/cyber security-is-hr-target

[15]. Where Digital Meets Human: Letting HR Lead Cybersecurity Training: By Jennifer Gregory: https://securityintelligence.com/articles/cybersecurity- training-hr-nontechnical-personnel/