Accountancy Business and the Public Interest
ISSN: 1745-7718

Volume: 39
Issue Number:08

THE PERSPECTIVE OF HR IN MANAGING CYBERCRIME AND CYBER SECURITY ISSUES IN THE INDIAN BANKING SECTOR

SREEKAR G.S.G

(Research Scholar), Department of Commerce and Management Studies, Andhra University, Visakhapatnam, Andhra Pradesh.

PADALA VISWANADHAM (Guide)

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

Abstract

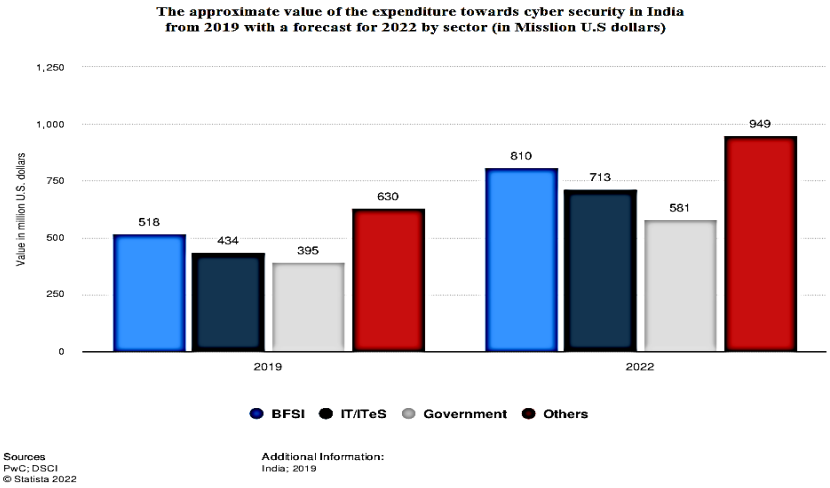
Background: Managing cyber security issues in any organization, particularly banks, is one of the key duties of any human resources (HR) department. By setting rigorous standards, spreading practical understanding, and ultimately constructing a vulnerable-free cyber security environment, the HR's involvement in managing cyber security challenges has been expanding by leaps and bounds. Because any carelessness might pose an immediate threat to the organization, a human resource manager plays a significant role in teaching both staff and consumers.

Keywords: Cyber hygiene, Cyber Security, Preventive Measures, Practical awareness, Managing issues, HR's role in cyber security

INTRODUCTION

Hiring the right cyber talent has become a challenging task to HR and in the first case the Human resource manager himself must have practical knowledge on cyber security. The employees consider Cyber Security as an IT related issue but it is not restricted to IT department, it the responsibility of every individual employee or customer of any organization particularly banks to learn how to manage cyber security issues in relationship with the banks as a customer or as an employee. Until one becomes victim to any cyber issue not one reacts and realizes the importance of cyber security knowledge.

According to a research, cyber security breaches can cost at least 200 billion dollars every year progressing further and therefore global spending on the name of cyber security also exponentially increases naturally in order to protect from the causative threats and manage the live issues.



LITERATURE REVIEW

The primary concern of a financial institution's security system like a bank was to secure its physical data and its buildings. But, in contrast, the continuously evolving technology has played a significant role in transforming the classical business functions to be highly sophisticated and facilitated the digital operations of banking industry. However, a highly technology-oriented institution may encounter an array of challenges, because of the lack of customer awareness and cyber illiteracy which can lead to information breaches and hackers' attempts to destroy crucial information. As a result, banks are required to be highly cautious and circumspective of such threats through the adoption of up to date cyber security systems to mitigate and control the cyber risks.

RESEARCH GAP

There's an enormous cyber security talent gap in the banking industry. The ever changing cyber threats have forced the necessity of cyber professionals in both public and private sectors and the requirement is not optimum.

With a lack of competent cyber security workforce, the organization becomes an easy target for hackers, leading to several damages including data breaches, loss of reputation, lack of profits, etc.

There has been no proper research on how and why Human Resources Department should be equally equipped with the right skills to recruit the right cyber security experts with the latest updated knowledge.

This research focusses on the importance of Human Resources Department in updating its knowledge in cyber security issues to recruit the right people and create awareness towards establishing cyber hygiene.

OBJECTIVES

The main objective of the study is to investigate into the role of HR in mitigating cyber security issues in the banks: Specifically, the study seeks to identify the HR's role in the following:

- HR's role in finding out the best solutions to the current cyber security issues
- Looking into the current challenges the HR department has
- Procuring enough budget for Cyber security in the banks
- Creating relevant policies
- Working parallel with the IT department
- Establishing proper training sessions
- Empowering employees with the right tools
- Strategy to create/spread awareness among the customers

The meaning of Cyber Security

The set of techniques, technologies, practices that can be followed to keep our systems, devices, transactions, data, online privacy safe from any type of intruders, hackers, cyber criminals or malicious attackers.

The importance of Cyber Security

Cyber security is vital in this generation as it protects all types, categories of information or data theft and damage. The information can include highly sensitive data, Identifiable ultra-personal information, highly confidential health information, intellectual property, financial information, important data which if falls in the hands of the unauthorized persons can lead to unprecedented loss. As the process of the digitalization is spreading very fast if an intelligent person has no knowledge he is vulnerable to cyber-attack at any point of time. Cyber-illiteracy or lack of Cyber security knowledge can land anyone in trouble. The knowledge of cyber security would lead the future world as cyber criminals keep finding their innovative ways to misuse any lacuna found in the security.

Cyber Security encompasses all types of data in this digital world. Having a sophisticated cyber defense mechanism, programmers in place to protect the sensitive data is very crucial in everyone's interest in the world. In this society almost all types of people rely on critical infrastructure, such as medical help from hospitals/health care institutions and financial services like banking to keep our society running. From the point of an individual, any type of cyber-attack can lead to sensitive identity theft and cyber bullying, extortion attempts which can cause serious damage to the individual's life.

We always rely on the safety of our data and personal information taking it for granted, to discuss a practical example, while logging into an application or while filling in the sensitive data like passwords, or a credit card pin, if the systems and networks and infrastructure have no protection, our crucial data would fall into the wrong hands.

In this sense, we must be well-versed with the ever-changing technological trends and policies. The government, big organizations, all types of businesses, the military and other socially critical entities must take latest, updated cyber security measures to prevent huge loss, as they store huge amount of data on online, computers and other types of devices.

Majority of this data comprises highly sensitive information. Any amount of exposure of this crucial data can be very harmful to businesses, personal reputation, customers' trust in the organizations, employees' responsibility etc.

Cyber Security, its importance and relevance in the Banking Industry

Banking industry is highly vulnerable as it is the first financial institution that is prone to vulnerability by all types of cyber-attacks. Any type of data breach can make the whole banking industry difficult to be trusted by its customers. Cyber threat can be a very serious issue, a weak security system can result in serious data breaches that can make its customers' base to withdraw trust and save/invest money elsewhere.

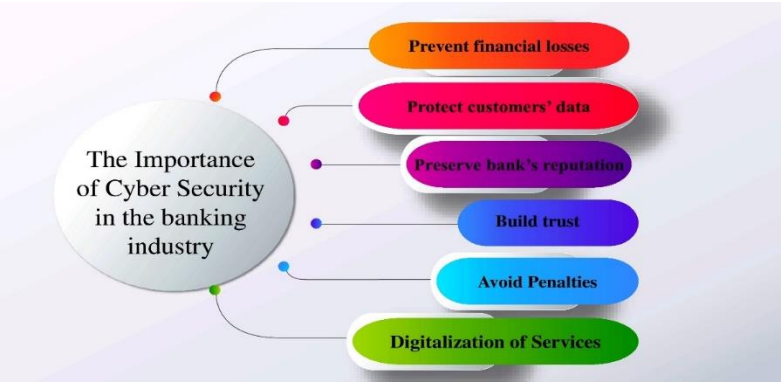
Everyone in this century seems to be going cashless, using digital money in the form debit or credit cards. In this regard it becomes very important to ensure that all types of measures are properly taken care of by establishing high priority standards.

Private sensitive data falling prey in the hands of cyber criminals can do great harm. Recovering the loss of money or data is not an easy task as easy as it appears to be, and even if the legality comes into picture, and tries to protect the customer as per the law, it is almost not possible to put the fraudsters, criminals behind the bars immediately.

The cyber criminals are concocting increasingly sophisticated techniques and designing highly effective or otherwise destructive malicious software (also known as malware) to escape antivirus detections. The best way to tackle such destructive threats is by understanding the very nature of the hackers and keeping our cyber awareness updated on the new attack evolving

techniques and scams being used. Having strict cyber security solutions in place will allow a bank to achieve it.

The below illustration shows the importance of Cyber Security in the banking industry



The Types of Challenges to a Human Resource Manager in the Banks

- The right Cyber talent gap
- Uninformed employees
- Lack of budget
- Weak credentials
- Mobiles devices and apps

The Solutions

- Identifying the right security partners
- Implementing continuous security awareness and training
- Continuous and Comprehensive assessment on the current programs
- Purchasing latest detection and response tools
- Carrying out highly practical and rigorous customer awareness programs.

CONCLUSION

Establishing practical cyber security defense mechanisms for banks might seem to be difficult task, especially from the Human Resources point of view as even any minute mistake can have severe repercussions. However, by establishing comprehensive training and security awareness sessions to the employees as well as the customers and creating strategic tools and competencies, hiring the right cyber-security talent, and implementing the right policies, banks can be secured from cyber-attacks.

The Human Resource department of a bank is responsible for not only updating employees' attitudes toward cyber hygiene but also making sure all the policies are strictly followed by continuous observation. Hence, the Human Resource department mustn't be complacent or compromise from focusing on the most trending, latest issues. After all, it is the responsibility of the HR department to make sure the entire bank employees/customers are complying by the security rules.

References

- Al-Alawi, A. I. (2005), Adoption and Awareness of Online Banking Issue among Mature Users. Asian Journal of Information Technology, 4(9) pp. 856-860.
- Al-Alawi, A. I., & Abdelgadir, M. F. (2006). An empirical study of attitudes and opinions of computer crimes: A comparative study between UK and the Kingdom of Bahrain. Journal of Computer Science, 2(3), pp. 229-235.
- Al-Alawi, A.I. (2014). Cybercrimes, Computer Forensics and their Impact in Business Climate: Bahrain Status. Research Journal of Business Management, 8: 139-156. [Online],
- http://www.scialert.net/qredirect.php?doi=rjbm.2014.139.156&linkid=pdf
- Al-Alawi, A. I., Mehrotra, A. A., & Al-Bassam, S. A. (2020). Cybersecurity: Cybercrime Prevention in Higher Learning Institutions. In Implementing Computational Intelligence Techniques for Security Systems Design (pp. 255274). IGI Global.
- Al-Alawi, A. I., Al-Bassam, S. A., & Mehrotra, A. A. (2020). Critical Cybersecurity Threats: Frontline Issues Faced by Bahraini Organizations. In Implementing Computational Intelligence Techniques for Security Systems Design (pp. 210-229). IGI Global.
- Al-Bassam, A.M (2018), Investigating the Factors related to Cybersecurity Awareness in Bahraini Banking Sector, (Master theses, Arabian Gulf University (AGU), Salmanya, Kingdom of Bahrain) and supervised by Prof. Adel Ismail Al-Alawi. Unpublished dissertation, available from AGU Library.
- Arlitsch, K., & Edelman, A. (2014). Staying Safe: Cyber Security for People and Organizations. Journal of Library Administration, 54(1), pp. 46-56.
- BBA and PWC (2014). The cyber threat to banking: A global industry challenge, [online], [Retrieved April 22, 2017]
- https://www.bba.org.uk/wpcontent/uploads/2014/06/BBAJ2110_Cyber_report_May_2014_WEB.pdf
- Cawley, J. (2017). The Impact of Cyber Attacks on the Banking System. [Online] [Retrieved December 22, 2017] https://wall-street.com/impact-cyber-attacks-banking-industry/
- Cuomo, A. M., & Lawsky, B. M. Report on Cyber Security in the Banking Sector, New York State Dept. of Financial Services, 2014. [Online], [Retrieved May, 22, 2017]
- https://cybersecuritylawandpolicy.files.wordpress.com/2014/05/new-york-state-department-of-financial-servicesreport-on-cyber-security-in-the-banking-sector.pdf
- ISACA (2017), CSX Cybersecurity Fundamentals Study Guide 2nd Edition– January 1, 2017 [online] [Retrieved April, 22, 2017]https://cybersecurity.isaca.org/csx-resources/cybersecurity-fundamentals-study-guide
- McGoogan, C. (2017), Cyber Attacks against Financial Services Cost Consumers 8bn, [online], [Retrieved April 22, 2017]http://www.telegraph.co.uk/technology/2017/02/27/cyber-attacks-against-financial-services-cost-consumers-8bn/
- McKendry, I., (2015). With New Tool, Agencies Close In on Formal Cyber Standards. American Banker, APR 9, 2015.[Online][RetrievedMarch,12,2017]
- http://www.cbaofga.com/uploads/4/1/3/7/41371065/with_new_tool,_agencies_close_in_on_formal_cyber_standards_ __american_banker.pdf
- Kuepper, J (2017) Cyber Attacks and Bank Failures: Risks You Should Know, 21-01-2017, available at: Countering Terrorist Activities in Cyberspace, Z. Minchev & M. Bangladesh (eds)
- Newman, R. C. (2006, September). Cybercrime, identity theft, and fraud: practicing safe internet-network security threats and vulnerabilities. In Proceedings of the 3rd annual conference on Information security curriculum development, ACM, pp. 68-78.
- Raghu Nathan, S.& Menon, N. (2011). Cyber Security Risk Management: Public Policy Implications of Correlated Risk, Imperfect Ability to Prove Loss, and Observability of Self-Protection. Risk Analysis, 31(3), pp. 497512.
- Online Trust Alliance (2014), 2014 Data Protection & Breach Reading Guide, [online], [Retrieved April, 11, 2017] https://otalliance.org/system/files/files/bestpractices/documents/2014otadatabreachguide4.pdf

- Scully, T. (2014). The cyber security threat stops in the boardroom. Journal of business continuity & emergency planning, 7(2), pp. 138-148
- Spalević, Ž. (2014). Cyber Security as a Global Challenge of the Modern Era. Sinteza 2014-Impact of the Internet on Business Activities in Serbia and Worldwide, pp. 687-692.
- Summerfield, R (2014). Banking system faces cyber threat. Financier Worldwide Magazine, August 2014 Issue. [Online], [RetrievedApril,22,2018] https://www.financierworldwide.com/banking-system-faces-cyberthreat#.W7dKcHszZdg
- UK Government (2017), Almost half of UK firms hit by cyber breach or attack in the past year Nearly seven in ten large companies identified a breach or attack, new Government statistics reveal, Press release, [Online], [Retrieved April 22, 2019] https://www.gov.uk/government/news/almost-half-of-uk-firms-hit-by-cyberbreach-or-attack-in-the-past-year
- VanBankers (2016). Cybersecurity in Banking. [Online], [Retrieved April, 22, 2017]
- www.vabankers.org/LiteratureRetrieve.aspx?ID=155390
- Vande Putte, D., & Verhelst, M. (2014). Cyber-crime: Can a standard risk analysis help in the challenges facing business continuity managers? Journal of business continuity & emergency planning, 7(2), pp. 126-137.