Cyber Security In Internet Banking

Abstract

Internet banking is one of the fastest and easiest way of banking. The threat of cyber security attacks is one of the very big challenges for internet banking and industries that are included in electronic commerce. In this report, we first analyze the cyber security in internet banking in detail and then an explanation of procedures and processes are undertaken for the investigation and research. The questions were based upon user’s knowledge about cyber security and user’s awareness of common threats in Internet banking. The results obtained support the argument that there is an emerging gap between banks' expectations and users’ actions related to internet banking(Jaafar, Zafar, Ghazanfar, 2017).

Introduction

Nowadays, cyber security is an important part of any kind of field that is related to the internet. It is the method or way to protect personal or important data from misuse or exploitation from any unintended access. So, basically, it is very crucial for each and every electric sector. Because, there are various hackers in the market that try to exploit the information and misuse them, there is a need to solve this problem. So, in this report, I would like to explain the role of cyber security in the banking sector, the role of IT in innovation and organizational success, the determination of research philosophies for IT projects and bank approaches and then the view about the IT sector that is contributing to banking sectors. And then it will explain the ability to find the significant resources, their familiarity. Moreover, it will explain the methodologies used in the research and its discussions and implications of the research.

Literature Review

Information technology plays a crucial role n the field of banking. It helps to protect the data from misuse and any unintended access. The software of cyber security is very helpful for the banks for protecting them from any problems. The Microsoft Security Intelligence Report indicates that the most common category of malware was worms and 8.3% of computers were affected. The different types of software that we use encryption. Encryption is the method of encrypting the data that changes the data in an encrypted form and a kind of protected from password This is a kind of security key that helps the data to protect with the help of password and encryption.

Another way is to connect all the devices with the technology and make sure it is protected. For e.g. CCTV cameras at the workplaces that are connected with the internet and technology and can keep records on phones. The other one is unprotected third-party services that show that the internet is a universal connector, therefore the unprotected third-party services can open the door for cyber attackers to access data. Therefore cyber security should be given connector when you connect services, rather than an afterthought.

Moreover, mobile banking applications should be secured and protected. And they are very

important and used by almost 95% of the people. And every person is totally dependent on mobile these days for their transactions and any other records. So the mobile banking should be protected from cyber threats. Because, in these days, everyone's bank accounts, their important ids and much other important information are connected to the mobiles.

Methodology

There are various kinds of techniques and methods available that are used for the investigations, research and data collection techniques and different kinds of techniques for decision making.

Data Collection

Data collection is a kind or a way of collecting or gathering the data for different kinds of purposes, such as for research, investigation, and some other purposes. There are different methods for collecting and gathering the data. The methods are given as follows:

Observation

Observation plays an important role in any kind of research. It is the most significant and common technique of data collection. Analysis of questionnaire responses is concerned with what people think and do as revealed by what they put on paper. The responses in interview are revealed by what people express in conversation with the interviewer. Observation seeks to ascertain what people think and do by watching them in action as they express themselves in various situations and activities.

Observation is the process in which one or more persons observe what is occurring in some real-life situation and they classify and record pertinent happenings according to some planned schemes. It is used to evaluate the overt behavior of individuals in the controlled or uncontrolled situations.. It is a method of research with the external behavior of persons in appropriate situations.

Observation means accurate watching, knowing of phenomena as they occur in nature with regard to cause and effect or mutual relations.

It mainly focuses on two points:

1. In observation, the observer wants to explore the cause-effect relationships between facts of a phenomenon.
2. Various facts are watched accurately, carefully and recorded by the observer(Poppe, Ziebland & Mays, 2000).

Interview

Interview as a technique of data collection is very popular and extensively used in every field of social research. The interview is, in a sense, an oral questionnaire. Instead of writing the response, the interviewee or subject gives the needed information verbally in a face-to-face

relationship. The dynamics of interviewing, however, involve much more than an oral questionnaire.

The interview is a relatively more flexible tool than any written inquiry form and permits explanation, adjustment and variation according to the situation. The observational methods, as we know, are restricted mostly to non-verbal acts. So these are understandably not so effective in giving information about a person's past and private behavior, future actions, attitudes, perceptions, faiths, beliefs thought processes, motivations etc.

The interview method as a verbal method is quite significant in securing data about all these aspects. In this method, a researcher or an interviewer can interact with his respondents and know their inner feelings and reactions. G.W. Allport in his classic statement sums this up beautifully by saying that "if you want to know how people feel, what they experience and what they remember, what their emotions and motives are like and the reasons for acting as they do, why not ask them".

The interview is a direct method of inquiry. It is simply stated as a social process in which a person known as the interviewer asks questions usually in a face to face contact to the other person or persons known as interviewee or interviewees. The interviewee responds to these and the interviewer collects various information from these responses through a very healthy and friendly social interaction.

However, it does not mean that all the time it is the interviewer who asks the questions. Often the interviewee may also ask certain questions and the interviewer responds to these. But usually, the interviewer initiates the interview and collects the information from the interviewee.

The interview is not a simple two-way conversation between an interrogator and informant. According to P.V. Young, "interview may be regarded as a systematic method by which a person enters more or less imaginatively into the life of a comparative stranger". It is a mutual interaction of each other(Attride, 2001).

Questionnaire

The questionnaire is the simple, easy and fast way to collect and gather data about groups of individuals scattered in a wide and extended field. In this way, a questionnaire form is sent to the group of people or persons concerned with a request to answer the questions and return the questionnaire.

Basically, the questionnaire is a kind of stimulation that creates an environment that is the same as a kind of questionnaire in which people predict themselves in that environment and then answer the questions.

On the other hand, the schedule is also a kind of method that is used to collect the data and is basically the same as a questionnaire that contains a set of questions and then people or the participants answer these questions.

Since the questionnaire is sent to a limited number of people but still it is the most effective technique to gather or collect the information. It can gather all the efficient information by

sending the questionnaire to a limited number of people.

Case Study Method

A case study is a form of qualitative analysis involving the very careful and complete observation of a person, a situation or an institution. It is a way of organizing social data so as to preserve the unitary character of the social object being studied. So in this way they send a case study with some questions to an individual or a group of individuals, then they study the case study and answer the questions according to their understanding and thoughts, it is also a good way of gathering the information.

Decision Making Techniques

First of all, decision-making is the way of making decisions that are good for the company or the organization. There are various kind of techniques that has been used for making good decisions. The following techniques are as follows:

- Operational Decision Making: Operational decisions are decisions made to manage day-to-day business. Any firm which is into any kind of business is faced with 100 decisions they have to take in a day. These will be as mundane as refilling the water cooler, to as stressful as fulfilling customer order within minutes. For e.g. in company-A, the managerial kind of decisions are like at the ground level, which manager will work or another day to day decisions. Company-A sets key performance indicators that help them to make day-to-day decisions.
- Tactical Decision Making: Tactical decisions are medium-term decisions usually spanning between six months and one year. Tactical decisions are made within the limitations of the overarching strategic supply chain decisions, in other words, they are planned towards accomplishing and executing the strategic level decisions. For e.g. in Company-A, tactical decisions are taken by the managers and with the help of the key performance indicators, that is based on the variances and general external information as well(Gardner, 2014).
- Strategic Decision Making: Strategic decision-making is the process of charting a course based on long-term goals and a longer-term vision. By clarifying your company's big picture aims, you'll have the opportunity to align your shorter-term plans with this deeper, broader mission – giving your operations clarity and consistency. For e.g. in company-A, the upper management would take these kinds of decisions, that are for the long term and strategic terms. So in this, managerial directors would take the decisions.

Discussion And Implications Of Research

There is a need of ethical clearance. As there are some threats of cybercrime in the banking sector, that it is important that the project would go in a responsible and ethical accountable way. It will make sure that all the things would go in the right way. It also helps to protect humans from any harm that can be caused by the project implications. Ethical clearance is also important to ensure that the research leads to beneficial outcomes. That the project that is going to implement does not harm the dignity, rights and safety of the research participants and that the research design is ethically sound and is likely to render the anticipated results.

It is also helpful to increase the legitimacy of the research findings for those making decisions based on the research results(Martyn, 2003). It would make sure that all the data that is in research would keep the data secure and private, no unintended access can be possible to steal the data of the research. It make sure that the information related to the identity of the researcher and its team would keep remaining private and secure. Just to make sure that no one can misuse it before the publishing of the research.

Moreover, cyber-attack is the deliberate exploitation of computer systems, technology-dependent enterprises and networks. Hackers (cybercriminals) use malicious code and software to alter computer code, logic, or data, resulting in disruptive consequences that can compromise data and lead to cyber-crimes such as financial information, healthcare record, and identity theft or system infiltration. So cyber security will help to solve these kinds of problems and it will make sure that all the data is secure and safe, nobody can access it without passwords and security keys(Lynn, 2004).

Customers' Accounts – Customer accounts can be the most vulnerable point of entry to a bank's systems. The hackers used stolen privileged credentials to steal from their accounts. So, cyber security will make sure that the information regarding the customer's account would be confidential and be secured. Cyber security installs biometrics in which customers' faces, thumbprints and eye locks are used as a password(Wilson, 2010).

Conclusion

In a nutshell, it concludes that cyber security plays an important role in each and every field. In the banking sector, there are various threats that can cause loss of confidential information,, so to protect the cyber security is very important, it helps to keep the data confidential and private. It basically focuses on security considerations that include internet banking, mobile banking, wallet transactions, ATM Security and unified Paytm interference. Furthermore, what is known about cyber security is often compartmented along disciplinary lines, reducing the insights available from cross-fertilization.

This primer seeks to illuminate some of these connections. Most of all, it attempts to leave the reader with two central ideas. The cyber security problem will never be solved once and for all. Solutions to the problem, limited in scope and longevity though they may be, are at least as much nontechnical as technical in nature.

References

1. Department of Homeland Security, A Comparison of Cyber Security Standards Developed by the Oil and Gas Segment. (November 5, 2004)
2. Gardner J. Ethical issues in public health promotion. S Afr J Bioethics Health Law2014; 7(1):
3. Grassi, P.; Garcia, M.; Fenton, J.;National Institute of Standards and Technology; U.S. Department of Commerce., Digital Identity Guidelines (800-63-3).
4. Guttman, M., Swanson, M., National Institute of Standards and Technology; Technology Administration; U.S. Department of Commerce., Generally Accepted Principles and Practices for Securing Information Technology Systems (800-14). (September 1996)
5. Martyn C. The ethical bureaucracy. QJM-Int J Med 2003; 96(5): 323–4.

6. National Institute of Standards and Technology; Technology Administration; U.S. Department of Commerce., An Introduction to Computer Security: The NIST Handbook, Special Publication 800-12.
7. Swanson, M., National Institute of Standards and Technology; Technology Administration; U.S. Department of Commerce., Security Self-Assessment Guide for Information Technology Systems (800-26).
8. Stouffer, K.; Pillitteri, V.; Lightman, S.; Abrams, M.; Hahn, A.; National Institute of Standards and Technology; U.S. Department of Commerce., Guide to Industrial Control Systems (ICS) Security (800-82).
9. Wilson J, Hunter D. Research exceptionalism. Am J Bioeth 2010; 10(8): 45–54. Do
10. Attride-Stirling J. (2001). ‘Thematic networks: an analytic tool for qualitative research’. Qualitative Research, vol. 1, no. 3: pp. 385–405 [Online]. Available at http://goo.gl/VpQeQJ (retrieved on 2 January 2014).
11. Pope, C., Ziebland, S., and Mays, N. (2000). ‘Analysing qualitative data’. Medical Journal, 320 : pp. 114–116 [Online]. Available at http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1117368/pdf/114.pdf (retrieved on 2 January 2014)
12. The Psychological Society, Code of Human Research Ethics (2010), http://www.bps.org.uk/sites/default/files/documents/code_of_human_research_ethics.pdf
13. ESRC, Framework for Research Ethics (2016), http://www.esrc.ac.uk/funding/guidance-for-applicants/research-ethics/
14. UK Clinical Ethics Network, Ethical Issues, http://www.ukcen.net/index.php/ethical_issues