Research paper on risk briefing paper

Business, Management

Introduction

With increased technological advance and globalization, businesses in different industries and sectors are increasingly adopting online business systems as platforms for reaching a wider market as well as enhancing their efficiency and effectiveness. In that respect, the banking industry has been in the forefront in rolling out innovative products and services. However, the development has been matched by growing crime activities like internet fraud and scams which pose significant risks to the industry and individual firms. In that consideration, this analysis seeks to demonstrate the risks the internet fraud and scams pose to the industry and how they can be managed by discussing the banking industry and JP bank's nature as well as the specific risk and its possible disruptions. Further, the analysis explains how the risk can be measured and managed as well as identifies those who should be responsible and the importance of such risks and management to the industry and the business.

- Overview

Business/Industry nature

The banking industry is marked by high risk products and services as well as rapid adoption of technology application in the market players operations. The key products and services in the industry and offered by JP bank include bank accounts, credit facilities, plastic money as well as money transfer services. In addition, the industry fall under the finance sector which has a complex web on interlink between the market players and their operating systems. (Ernst & Young, 2012) In that respect and consideration of the

global nature of the finance sector, the industry is marked by a fast growth and adoption of technology and related advances in a bid to enhance service delivery, efficiency and market reach. It is that need to reach the global market and connect the industry systems through application of web based products and solutions that expose it and the operators to great risks including internet frauds and scams. (MasterCard, 2013)

Risk nature

Frauds and scams mainly include activities like money laundering, theft and embezzlement all of which are easily carried out on an online platform through the internet. (CIMA, 2013) Further, frauds and scams may include crimes committed by outsiders including clients and business partners on a business or by employees on the employer who on this case refers to the banking institutions. Such crimes include information/data and cash theft, assets misallocation, as well as theft of intellectual property. However, for the purpose of this analysis, the risk that will be focused on the fraud and scams that seek to steal cash out of bank. (CIMA, 2013)

Possible disruptions

In respect to the fraud in focus, the possible disruptions in the industry and to the bank in specific would be perpetrated through the fraudsters' access to clients' accounts. (JPMorgan, 2013) Such theft would result into loss of funds to the customers. Further, an occurrence of a serious fraud on a banking institution could even result to the institution's closure by the relevant authorities are meant to ensure that clients' funds are secure. (FBI, 2013)

- Risk measure

Risk involving internet frauds and scams in the banking industry are closely related to cybercrimes and cash theft. In that respect it is easier to measure the risk involved by identifying the amount that could be exposed to such unauthorized access. (MasterCard, 2013) In addition, identifying the amount involved in attempted fraudulent activities can in itself be a clear reflection of the risks involved. A good example was the measure of the risk to which the European market banking industry was exposed to in 2010 through cybercrimes that targeted $75 million. However with the development advanced online banking malware the amount at risk in the European market in the year 2011 significantly increased to an estimated figure of $2. 5 billion. (Constantin, 2012)

- Risk management

In respect to increased risk that relate to internet frauds and scams in the industry, the risk management that should be applied in the by the specific companies and the industry player in general should follow the process of

- Establishing management objectives and goals in respect to the risk management
- Identification of key risk factors.
- Assessing the risk.
- Developing suitable strategies for risk response.
- Allocating and implementing the strategies
- Monitoring and controlling the implementation
- Review of the strategies effectiveness and adjusting as the situation demands (CIMA, 2013)

At the industry level and with specific companies, some of the risk management strategies that could effectively address the problem include

- Developing high industry standards for high risk services and products like electronic transfers and payments. (Kerry, 2013)
- Enhancing collaboration among the stakeholders.
- Application of best practices and leadership. (Ernst & Young, 2012)
- Development of effective IT governance that has strategies encompassing effective organizational structures, leadership, business processes, compliance and standards. (Wakely, 2003)
- Further, banks should undertake to educate their key stakeholders including customers and suppliers on the risks involved with the banking transactions and products. (MasterCard, 2013)
- Responsibility in risk management

In respect to the risks involved with internet frauds and scams that target cash theft in the banking industry, responsibility to manage the risks cuts across a wide range of including banks and their employees, bank customers and partners as well as the regulatory authorities. (Stewart, 2000) The regulatory authorities involved should seek to ensure that a bank meets industry standards in terms of system security. (Dorgham, 2013)

- Importance of the risk to banking industry and JP bank

In respect to the risk that is posed by internet fraud and scams that target cash and bank data theft, the industry and JP bank in specific needs to put good control measures. (Wakely, 2003)

- Avoiding or reducing financial loss.
- Avoiding customer loss hence fostering growth for specific institutions and

the industry in general.

- Fostering adoption of advanced technology like online banking and transactions. (MasterCard, 2013)

Conclusion

In light of the discussion, it has been demonstrated that banking industry faces high risks in terms of internet frauds and scams that target data and cash theft. Thus, it is paramount for the industry stakeholders to establish risk management strategies that effectively address the problem in order to avoid possible disruptions that could include loss of customers and funds as well as loss of trust in advanced online systems.

Reference list

CIMA. 2013. Fraud risk management: A guide to good practice. [Online] Available at

[Accessed 09 September 2013]

Constantin, L. 2013. Cybercriminals increasingly use online banking fraud automation

techniques. Computerworld. [Online] Available at [Accessed 09 September 2013]

Dorgham, M . A. 2013. Principles and theory of Risk Assessment and Management.

International Journal of Risk Assessment and Management. ISSN Online: 1741-5241.

Ernst & Young. 2012. Top and emerging risks for global banking. [Online] Available

at [Accessed 09 September 2013]

FBI. 2013. Common Fraud schemes. [Online] Available at

[Accessed 09 September 2013]

JPMorgan. 2013. Cyber source: 2012 online fraud report. [Online] Available at

[Accessed 09 September 2013]

Kerry, J. 2013. Risk Management: Lessons Learned from the financial Crisis: One CRO’s

View. Journal of Risk Management in Financial Institutions. Vol. 6(2): (2012-13), ISSN (web): 1752-8895.

MasterCard. 2013. Advancing fraud management for more secure payments. [online]

Available at

[Accessed 09 September 2013]

Stewart, F. 2000. Internet Acceptable Use Policies: Navigating the Management, Legal, and

Technical Issues. Information Systems Security. Vol 9(3): pp. 46-53.

Wakeley, N. 2003. Internet Banking Fraud Investigations. GIAC Security Essentials

Certification (GSEC) Practical Assignment V1. 4 Option 2 Case study. [Online]

Available at

[Accessed 09 September 2013]