Risk management briefing paper essay

Business, Management

\n[toc title="Table of Contents"]\n

\n \t

\n[/toc]\n \n

Introduction

The banking industry is a major target of the increasing levels of Internet fraud and scams. With the advancements in technology, cybercriminals have developed more sophisticated tools for stealing money from banks, which can result in millions of dollars of financial losses for these banks (Constantin 2012).

For Secure Future Savings Bank, in particular, Internet fraud and scams can disrupt its online banking operations. With online banking being so popular among Future Savings Bank’s customers due to the convenience and ease it brings them (Why is online banking is so popular these days? n. d.), disruptions in these operations can result in decreased customer satisfaction and decreased customer trust. In particular, these operations include electronic fund transfers, bill payments, and other account management tools that the customers use to manage and maintain their bank accounts.

Risk Measurement

One way to measure this risk is by determining the robustness of the physical, technical, and administrative controls (Chapter 1: Fundamental Security Concepts n. d.) that are in place for preventing the occurrence of Internet fraud and scams. Another way is by determining the level of the organization's compliance to these established controls (Measure and Reduce Risk 2013). By determining the level of compliance, it will be possible to identify the departments or teams where the risk may occur and it can help determine gaps in the organization's guidelines or controls, which need to be addressed in order to prevent the risk from occurring. In addition, the risk can be measured by performing an IT audit, which is an audit of the organization's IT systems, operations, management, and related processes (Auditor-General's Office 2009)

Risk Management

The risk of Internet fraud and scams can be managed by implementing controls that would enable the prevention of such. Some of these controls include implementing rigid guidelines for ascertaining the true identity of the individual customers or the commercial enterprises that the bank conducts business with and having an adequate monitoring system that would identify suspicious transactions (BITS 2003). In particular, reports can be used for monitoring transactions that go into and out of deposit accounts and for monitoring large deposits. In addition, systems should be in place for the real-time monitoring and validation of online transactions.

Moreover, a limitation should be imposed on the timeframes during which an application is completed. This can prevent thieves from keeping an

application open while they research customer data. In the same manner, a limit should be implemented on the length of time before a customer is automatically logged out of the system due to inactivity (U. S. Bank 2013). Similarly, a secure channel should be provided for the receipt of the customer's data; thereby preventing the interception of the said information. An audit trail should also be created. This includes the capture of the time and date when transactions are made, as well as the IP address of the user who made the transaction. This can help in authenticating the user when he or she makes another transaction.

In the same manner, a real-time process must be implemented for determining if a customer is providing an accurate representation of himself or herself. In particular, a system that has automated identity-verification and fraud-detection processes should be in place. As well, Secure Future Savings Bank can partner with third party providers of pattern recognition services, such as Web environment tracking, which prevents a thief's overuse of the system, and false address tracking, which monitors the number of times that the same address is used with various Security numbers and last names. Moreover, these third part service providers can provide various data checkpoints (e. g. checking the validity of Social Security numbers and addresses) and can use external options for further verification (e. g. running the customer's data against a database of ongoing fraudulent activities).

Risk Management Responsibility

The main responsibility for managing the risk of Internet fraud and scams will lie with the CIO or the Chief Information Officer. The CIO reports to the

Chief Executive Officer and is mainly responsible for the computer systems and information technology that support the bank's goals (Schneider 2013). More specifically, the CIO shall be responsible for establishing and implementing the controls necessary for protecting the bank's system, although he or she will need to delegate the making of technical decisions to the employees who are more familiar with the details. Since the CIO is responsible overall for the design, implementation, and use of the bank's IT resources, he or she shall also be responsible for devising strategies that would keep these resources secure and that would prevent disruptions in the bank's online banking services.

Importance of the Risk to the Organization and the Industry

It is important for Secure Future Savings Bank and the entire banking industry to address the risk of Internet fraud and scams because these can lead to financial losses. They can also decrease sales; cause the bank's reputation to be damaged; for the customers to lose their trust in the bank; and for the investors to lose their confidence in the bank (How Bad Could It be? n. d). In addition, they can lead to losses in the resources used for managing fraud incidents and possible legal costs. As well, they can decrease employee morale and can decrease the value of the bank's stock and services. Although Internet fraud and scams cause operational risks, such as the disruption of the bank's online banking services, these operational risks can lead to other types of risk, such as strategic risks, market risks, and reputational risks (Global Association of Risk Professionals 2013).

References

Auditor-General's Office, 2009. What is an IT audit? [online] Available at: < http://www. ago. gov. sg/doc/r39d. pdf> [Accessed 2 September 2013].

BITS, 2003. Fraud prevention strategies for Internet banking. [online] Available at: [Accessed 2 September 2013].

Chapter 1: Fundamental security concepts, n. d. [online] Available at: < http://www. mhprofessional. com/downloads/products/0072254238/0072254238_ch01. pdf> [Accessed 2 September 2013].

Constantin, L., 2012. Cybercriminals increasingly use online banking fraud automation techniques. [online] Available at: < http://www. computerworld. com/s/article/ 9228527/Cybercriminals_increasingly_use_online_banking_fraud_automation _techniques> [Accessed 2 September 2013].

Global Association of Risk Professionals (GARP), In: Operational risk management. Chap. 12. [online] Available at: How bad could it be? The effects of online fraud, n. d. [online] Available at: < http://www. onlinefraudguide. com/effects-online-fraud/> [Accessed 2 September, 2013].

Measure and reduce risk, 2013. [online] Available at: < http://www. hisoftware. com/solutions/by-need/measure-and-reduce-risk. aspx> [Accessed 2 September 2013].

Schneider, L., 2013. CIO - Chief information officer: All About the role of a CIO. [online] Available at: < http://jobsearchtech. about. com/od/careersintechnology/a/CIO. htm> [Accessed 2 September 2013].

U. S. Bank, 2013. Fraud prevention. [online] Available at: [Accessed 2 September 2013].

Why is online banking so popular these days? [online] Available at: < http://www. microfinancecongress. com/why-is-online-banking-is-so-popular-these-days/> [Accessed 2 September 2013].