Mastercard risk assessment

Technology, Information Technology

MasterCard Risk Assessment al Affiliation: Implementing risk assessment methodologies in this case scenario would entail an approach that suits the requirements and culture of the MasterCard Organization. This particular approach ought to exploit the subsequent discovery of the procedures that allow the MasterCard Company to discern harmful threats and mitigate them in a proactive, practical and well-timed technique. The risk assessment method that would be advisable is the MasterCard BRAM (Business Risk Assessment and Mitigation) program.

Utilizing this program would go long way in ensuring that the integrity of the payment platform or system is preserved. BRAM (Business Risk Assessment and Mitigation) program addresses all the illegal and damaging activities that are affiliated to the use of MasterCard. The program offers and delivers appropriate compliance standards required for safeguarding the use of the company’s services. Risk management usually promotes cost cutting in terms of insurance costs and operational costs that any financial organization often deals with when it comes to identifying and curbing fraud within the MasterCard financial systems (King, 2001).

The BRAM (Business Risk Assessment and Mitigation) program was developed by the MasterCard Company in order to minimize the industry and economic risk that comes with the use of MasterCard branded and affiliated cards. One of the economic risks posed on the system include the loss of clients who are not satisfied with the system operation, which subsequently leads to revenue loss for the firm. Addressing end user reliability of the MasterCard system is a vital objective for the MasterCard Company. System reliability can be achieved via ensuring there is constant testing and regular

monitoring of the network system.

The program warrants compliance through mandating and encouraging access control measures for the network system. Implementing and maintaining a strong security policy aids in protecting the clients information by boosting data security through the management of network systems utilized by the company and safeguarding then from unauthorized access (Gibson, 2004). Additionally, the set policies should limit any form of compromise that would arise even within the company itself, for example, selling of insider information.

The payment card industry has common industrial risks for all the companies that deal in payment systems using cards, that is, ensuring constant information security and availability of services or resources to subscribes at all times and places. The BRAM (Business Risk Assessment and Mitigation) program sets in place control objectives which govern the use of the MasterCard system by all the partners, merchants and individual clients. Moreover, the program provides strategies that promote comprehensive risk assessment and subsequently deliver investigation and resolution processes through establishing accountability within the organization (Siegel, Sagalow & Serritella, 2002).

The foundational controls mandated by the described policy informs the system end-users regarding the appropriately regarding any potential security flaws and advices them accordingly n how to keep their vital and personal information safe. This helps in minimizing any potential causes of data or information theft form the system. This information can be delivered to the users via disclaimer forms and email notifications that offer

informative data on rules that govern the use of the MasterCard network system (Wheeler, 2011).

Conclusively, the long term business operation of the MasterCard Company should be subjected to an external technology firm that has an extensive experience in dealing with risk assessment and prevention for the PCI (Payment Card Industry). Rotating methodologies has proven to minimize security breaches on a system, for example, if the MasterCard firm uses an information security firm in one particular year, for example, VeriSign which offers data encryption services and secured socket layers for data and network communication. In other years, the firm can use Qualified Security Assessor and vice versa. I strongly agree the company must protect consumer card data and information in accordance with the business set objectives and policies. Failure is not an option.

References

Gibson, C. F. (2004). IT-enabled business change: an approach to understanding and managing risk.

Siegel, C. A., Sagalow, T. R., & Serritella, P. (2002). Cyber-risk management: technical and insurance controls for enterprise-level security. Information Systems Security, 11(4), 33-49.

King, J. L. (2001). Operational risk: Measurement and Modeling. New York: Wiley.

MasterCard International SWOT Analysis. (2004). Datamonitor Plc.

Wheeler, E. (2011). Security risk management: Building an information security risk management program from the ground up. Amsterdam: Syngress.

Young, C. S. (2010). Metrics and methods for security risk management. Amsterdam: Syngress/Elsevier.