Risk Management for a Retail Business

Md Haris Uddin Sharif, Ripon Datta

***Abstract*—when creating a new company, there are various factors which should be considered by the management. Some of these issues range from the abilities to create a reliable approach for improving the insight into the operations carried out on a day to day basis. There exist multiple factors which may undermine the abilities of a new company to operate. Other than the business risks, other factors which should be considered may revolve around the technological challenges. Companies today are operating in an environment which is marked with various challenges such as cyber-attacks [5]. The inability of the management to create a platform for improved insight into the issues arising from cyber security may reduce the success rate of such a firm. Additionally, when considering the abilities of a company to maintain the desired level of operations, the efficiency of the underlying systems remain critical [2].**

***Index Terms*— management, cyber-attacks, efficiency.**

I. Introduction

The success of such a firm may be undermined by the lack of the right measures which would be used to support day to day growth and operations. The continued occurrence of cyber threats may undermine the abilities of a company to continue and supports its business operations. Sometimes, companies fail to implement the right measures which would be used to counter cyber threats and risks. In such a case, it is worth noting that the reduced insight of companies as far as the level of knowledge about cyber threats is concerned reduces the possibilities of firms to succeed in the industry and markets. Successful companies over the years have implemented measures which focus on the improvement of the level of operations [10]. One of the ways that have helped companies to achieve the desired level of growth and operations revolves around the introduction and implementation of technologies.

There exist multiple technologies that the new retail shop can use and apply to achieve better outcomes. The new firm may need to implement technologies which will help it to manage data within each store. Further, the firm may benefit from technologies such as cloud computing. These technologies create a platform for the improvement of the level of performance exhibited by the entity [3].

However, it is essential to note that the implementation of these systems may be subject to various challenges as far as cybersecurity is concerned. Today, a lot of companies continue to suffer from attacks which undermine their operations. Cyber-attacks are some of the significant threats and challenges which undermine the abilities of the respective entities from operating and undertaking their day to day operations. With the increased level of adoption of technology, companies need to perform a high-level risk assessment to seal the available weaknesses before an attack or a disaster happens [4].

When considering the ideas of risk analysis and management, companies should look at the aspects of resilience. To create a resilient operating environment, the company will need first to gain insight into the main weaknesses which its systems and architecture exhibits. To build a reliable cybersecurity plan, it is crucial for the management through the relevant stakeholders to create a reliable approach for identifying, analysing and mitigating the potential risks and threats that may occur in the future [7]. Such an approach would help the company to prepare for the occurrence of the unforeseen future events hence reducing the impacts. There are four main approaches that the management would need to implement after identifying and analysing the risks. These approaches are retained, share or transfer, reduce or mitigate and avoid, which involves elimination. Therefore, this project will look at the case of the identification of the main risks which the new retail would need to handle in the preparation of a cyber security plan. The failure to identify these risks will reduce the abilities of the firm to succeed in its operations.

II. The Need for Risk Management

Before embarking on the establishment of the business, the management needs first to understand some of the major challenges which it may face in the future. The primary type of challenges which may arise comes from the risks associated with the use of the associated systems and information technology solutions. To perform its operations, the business is likely to face a set of risks and challenges which will limit its abilities to achieve the desired levels of outcomes.

The primary role played by risk management comes from the abilities of companies to identify the various perils which may occur affecting their operations in the future. After identifying the risks, the next step involves understanding the implications of such perils on the day to day operations. For example, risk such as cyber-attack or hacking may involve unauthorized access of the internal systems and information by external or internal players. The main effect that this risk may bring to the company is a loss of data and negative perception by the general consumers as far as the corporate image is concerned.

Through the analysis of the main risks which may occur, it is important to look at the best ways to handle such perils. The creation of a conclusive cyber security plan requires a

Md Haris Uddin Sharif, Information Technology, University of the Cumberlands, Williamsburg, Kentucky
Ripon Datta, Information Technology, University of the Cumberlands, Williamsburg, Kentucky

company first to identify the main risks which may occur and then define the best interventions to implement in the course of operations. Companies usually fail to create the right mitigation strategies based on the lack of sufficient insight and knowledge about the effects of the underlying risks.

Primarily, the leading role of performing risk management and assessment process is to identify the potential challenges that may occur, affecting the operations of the underlying firm [14]. In this context, it is vital for the management first to identify the main risks which may occur and then develop a resilient plan. In the process, the ability of the company to create a reliable approach as far as risk management is concerned will come from the success in analysing some of the major perils and hazards which can occur in the course of operations affecting the underlying information systems. Failing first to identify these risks will undermine the abilities of the firm to create a reliable cyber security plan [11].

The need for a risk assessment and management plan helps to document the state of the current information systems as far as the creation of a platform for improved preparedness is concerned. Initial and prior preparations play a crucial role in cybersecurity planning because it helps in the development of additional mechanisms for handling the potential challenges that may occur on the day to day basis. After looking at the need for risk assessment and management, the following section outlines some of the major risks which the firm may encounter and then develops a set of recommendations which the management will need to document as far as the cyber security plan is concerned.

III. Encountered Risks

When it comes to the identification of risks, it is vital to use the right tools and techniques, which in turn will help in the improvement of the overall level of operations for the affected firms. There exist multiple enterprise risk management techniques and tools that can be used to overcome these challenges. In this context, it is worth using the right tools and techniques to gather data about the potential risks which may occur in readiness for the creation of a comprehensive cybersecurity plan.

IV. Tools and Technique

A. *Figures and Tables*

Some of the most common tools and techniques which have been sued over the years to aid in the collection of data about risks that may occur affecting the operations of the underlying systems and hence organization. Some of the most common techniques are brainstorming, SWOT analysis, risk questionnaires or surveys, scenario analysis and but not limited to interviews as well as self-assessments. The primary role played by these techniques comes from the idea that they all focus on the collection of data about the operations of a given firm looking at the aspects of weaknesses which the underlying systems exhibit.

These techniques play a crucial role in the creation of the ultimate platform for an improved level of insight into the major challenges and weaknesses that the underlying systems exhibit [13]. A SWOT analysis, for instance, helps to explore the internal and external strengths and weaknesses which a given firm exhibits. When applied in the context of risk management, this tool is essential in gathering the strengths, weaknesses, opportunities and threats that a given set of systems exhibits. It is worth noting that the use of these techniques and tools helps in the collection of data about the possible risks that may arise in the course of operations of a company. Therefore, these techniques and tools are essential in the risk assessment processes since they help to collect sufficient data from multiple dimensions and stakeholders. More information translates into better insight into the current state of the underlying systems as far as weaknesses and vulnerabilities are concerned.

Other tools which can be used in risk assessment and management include qualitative, rankings and but not limited to probability and impacts. These tools help in the analysis of the collected risks, which, in the process, facilitate decision making. For instance, a qualitative analysis helps to provide a theoretical explanation of the context of the risks identified. Further, ranking helps to assign the collected risks to a given rate based on the frequency of occurrence. Further, the impact and effect are numeric metrics which help in further classifying risks according to their priorities. In this context, the collective use and application of these tools and techniques help to obtain a comprehensive report about the nature of risks, rank, categories, potential impacts and frequency of occurrence. This information plays a crucial role since it helps to prioritize the risks identified to facilitate decision making on the best mitigation strategies to implement. Addressing the risks

V. Identifying the Risks

From the information given in the previous section, the company seeks to establish 10 new shops. However, the management is concerned about the potential risks which may occur affecting the company`s information systems. It is, therefore, worth identifying some of the main risks which may occur affecting the operations of the firm. This analysis will help in facilitating the development of the corporate cybersecurity plan to reduce the potential occurrence of unforeseen future events in the workplace.

Some of the most common risks that the company will need to focus on include hardware and security failures, malicious attacks, natural disasters, human error and but not limited to viruses. These risks may ring about diverse challenges to the company in case they occur [8]. To gain an understanding of the occurrence of the risks, it is important to explain them in details and then create a register. A risk register helps to combine various attributes such as the probability and impact of the perils identified to facilitate ranking according to the respective priorities. The risks with the highest priority exhibit high probability and impacts in case of occurrence.

VI. Viruses and Malicious attacks

Each company which operates information technology solutions and systems stands at a chance of suffering from various forms of risks. These risks in this context may come from viruses and malicious attacks. Malicious attacks usually involve the risks which come from unauthorized parties who try to gain access to a given information system or network for personal reasons and purposes. One of the leading examples which represent malicious attacks is a virus invasion. Viruses usually bring about diverse and adverse effects on the operations carried out by the respective companies.

When such an incident occurs, it is likely to corrupt or steal valuable corporate data. Attackers usually steal corporate data for their gains driven by diverse forces. Such an incident may target sources such as the servers and databases for the company. The occurrence of this form of incident risks the credibility and confidentiality of the corporate data. Many companies have continued to suffer virus and malicious attacks over the years, leading to diverse challenges such as loss of data, reputation and federal litigations [1].

VII. Human Error

The second most common risk which may occur affecting the operations of the retail store is human errors. Human errors may either be intentional or accidental. For instance, human errors may include an employee holding the door when entering restricted areas such as server rooms to unauthorized personnel. In such a case, the main effects would be a loss of data or compromise of the internal systems, which affects the integrity of information and the corporate systems. From another perspective, human errors may occur when employees open malicious and phishing emails sent by attackers unknowingly leading to data breaches [8]. In such incidents, the company needs to create the right measures to prevent the occurrence of such an occurrence. In the data environment, every business needs to put considerable focus on securing, creating a conducive infrastructure, and ensuring that Information is efficiently and accurately governed [15].

VIII. Natural Disasters

Thirdly, the company may suffer from natural disasters. Natural disasters may affect the operations of the company based on the magnitude of the effects and impacts of such occurrences. For instance, if a natural disaster such as floods, fires or earthquakes occur, they may negatively affect the operations of the company and the associated shops due to the massive destruction of equipment and systems. Natural disasters usually carry many magnitudes as far as the potential effects of damage are concerned on the underlying systems. Natural disasters usually require extreme care and attention when it comes to planning for the mitigation approaches to use and apply.

IX. Software and Haridware Failure

From another dimension, the firm may suffer from challenges such as software and hardware failures. These issues may arise from the breakdown of hardware components such as servers, routers and but not limited to workstations. When such an incident occurs, the company may suffer losses in the form of financial gains since such an event translates into downtime. Increased downtimes lead to loss of consumers. The reduced consumer brings about low profits. This undermines the abilities of a company to succeed in the future. From another perspective, software failures may be as a result of the use of counterfeit products or compatibility issues. Such events may result in reduced abilities of the retail shops to operate according to the desired levels of operations hence undermining the profitability of the firm [9].

X. Recommended Mitigation Strategies

From the analysis given above, it is crucial to create the right mitigation recommendations which will act as the ultimate solutions to reduce or manage the occurrence of such events. For instance, to mitigate the problems brought about by malicious attacks and viruses, the company will need to implement solutions such as intrusion detection and protection as well as antivirus systems. These systems will help to reduce the chances of malicious attacks in different forms such as malware and viruses [1]. The use of these approaches will help the company to reduce the risks of the occurrence of malicious attacks. Malicious attacks have a high probability and high impact in case of occurrence.

On the other hand, human errors have a high likelihood of occurrence and a high impact on the operations of a business. In case such an incident occurs, it may lead to a wide range of exposure of the corporate systems hence undermining the confidentiality of the company`s data and solutions. Further, human errors may lead to adverse effects such as phishing and intrusion from unauthorized personnel [8]. To overcome this problem, the company will need to subject the employees to a high level of training. Further, the firm will need to implement surveillance measures to continually monitor the people entering crucial areas such as server rooms and data centres.

From another dimension, natural disasters can occur at any time affecting the normal operations of the company. It is not possible to prevent the occurrence of incidents such as hurricanes or floods. However, the company should ensure that it creates a backup of its data and information. Further, to ensure resilience, the firm should operate another site which would be activated after the occurrence of a natural disaster. Maintaining a regular backup mechanism would reduce the risks of loss of data [6]. It is important to note that natural disasters have a low probability but high impact of occurrence.

Finally, software and hardware failures may occur, affecting the operations of the firm. These failures have a medium probability and medium impact on the operations of a firm. Software failures can be prevented by obtaining genuine copies of the products used. Further, maintaining a

team of experts from within the company would help to continually assess the potential risks of failures of the software and hardware products used. Moreover, SaaS as a stronger security can be use to build modern secure application [12].

XI. Conclusion

From the analysis given, some risks have a high probability of occurrence. On the other hand, some of the risks have a high impact rate. The company should ensure that it implements the right measures to reduce the potential occurrence of these risks. The company, in this context, should create measures which seek to avoid the occurrence of the risks. Risk avoidance remains one of the best approaches in the management of perils. The primary reason for this conclusion is that risk avoidance reduces the chances of the occurrence of the risks as opposed to building measures to handle such events. From another dimension, planning for the company as far as cybersecurity is concerned will require the management to understand the majority of the risks which may occur in the future. This project outlined that there are various risks which may occur inhibiting the operations of the firm.

After establishment, the management should focus on the creation of the ultimate platform for improving the operations carried out on a day to day basis through first performing a detailed risk assessment of the underlying systems. Risk assessment helps to provide a platform for improved knowledge about the main weaknesses which may arise in the systems implemented. The ability of the company to implement the proposed recommendations will determine its success in the future. Therefore, this project concludes that for the new retail stores to operate according to the desires of the management and owners, it is crucial to perform a high-level risk assessment and implement the proposed recommendations offered above.

References

[1] Apriliana, A. F., Sarno, R., & Effendi, Y. A. (2018, March). Risk analysis of IT applications using FMEA and AHP SAW method with COBIT 5. In 2018 International Conference on Information and Communications Technology (ICOIACT) (pp. 373-378). IEEE.

[2] Berry, C. T., & Berry, R. L. (2018). An initial assessment of small business risk management approaches for cybersecurity threats. International Journal of Business Continuity and Risk Management, 8(1), 1-10.

[3] Callahan, C., & Soileau, J. (2017). Does enterprise risk management enhance operating performance?. Advances in accounting, 37, 122-139.

[4] Fraser, J. R., & Simkins, B. J. (2016). The challenges of and solutions for implementing enterprise risk management. Business Horizons, 59(6), 689-698.

[5] Hopkin, P. (2018). Fundamentals of risk management: understanding, evaluating and implementing effective risk management. Kogan Page Publishers.

[6] Javaid, M. I., & Iqbal, M. M. W. (2017, April). A comprehensive people, process and technology (PPT) application model for Information Systems (IS) risk management in small/medium enterprises (SME). In 2017 International Conference on Communication Technologies (ComTech) (pp. 78-90). IEEE.

[7] Kohnke, A., Sigler, K., & Shoemaker, D. (2017). Implementing cybersecurity: A guide to the national institute of standards and technology risk management framework. CRC Press.

[8] Kumar, P., Gupta, S., Agarwal, M., & Singh, U. (2016). Categorization and standardization of accidental risk-criticality levels of human error to develop risk and safety management policy. Safety Science, 85, 88-98.

[9] Saeidi, P., Saeidi, S. P., Sofian, S., Saeidi, S. P., Nilashi, M., & Mardani, A. (2019). The impact of enterprise risk management on competitive advantage by moderating role of information technology. Computer Standards & Interfaces, 63, 67-82.

[10] Soltanizadeh, S., Rasid, S. Z. A., Golshan, N. M., & Ismail, W. K. W. (2016). A business strategy, enterprise risk management and organizational performance. Management Research Review.

[11] Tupa, J., Simota, J., & Steiner, F. (2017). Aspects of risk management implementation for Industry 4.0. Procedia Manufacturing, 11, 1223-1230.

[12] Sharif MHU, Datta R(2019). SOFTWARE AS A SERVICE HAS STRONG CLOUD SECURITY. Retrieved from URL: https://www.researchgate.net/profile/Haris_Sharif/publication/335232826_Software_as_a_Service_has_Strong_Cloud_Security/links/5d6466fc299bf1f70b0eb0f2/Software-as-a-Service-has-Strong-Cloud-Security.pdf

[13] Sharif MHU, Datta R,. Valavala M.(2019). Biometrics Authentication Analysis. International Journal of Mathematics Trends and Technology (IJMTT) – Volume 65 Issue 10 - Oct 2019 http://www.ijmttjournal.org/Volume-65/Issue-10/IJMTT-V65I10P506.pdf

[14] Sharif MHU, Datta R, (2019).BRING YOUR OWN DEVICE (BYOD)PROGRAM. International Journal of Engineering Applied Sciences and Technology, 2019 Vol. 4, Issue 4, ISSN No. 2455-2143, Pages 36-40. DOI : http://www.ijeast.com/papers/36-40,Tesma404,IJEAST.pdf

[15] Sharif MHU, Datta R, (2019). Information Governance: A Necessity in Today's Business Environment. IJCSMC, Vol. 8, Issue. 8, August 2019, pg.67 – 76. From url: https://www.academia.edu/40224559/Information_Governance_A_Necessity_in_Todays_Business_Environment_

Md Haris Uddin Sharif is a Ph.D. student of Information technology at the University of the Cumberlands. His research interest includes Cyber Security, Cloud Technology, Cloud Security, Application Development, Application Framework, Blockchain and Data Security. In addition to these, he engaged in research activities throughout his Ph.D. program and has several research papers (IJCIT, SCI-INT, IJERM, IJEAST, IJMTT, Research Gate, IJEAS and other).

Ripon Datta, Ph.D. candidate at the Department of Information Technology, University of the Cumberlands, Kentucky, United States of America. He is also a Senior Software Engineer in a Financial Corporation in the United States. Mr. Datta's research interest includes Software Development, Blockchain, Machine Learning, Application Security, Algorithm, etc.