**Introduction**

ACME Manufacturing is a small company in a niche field that is currently going through a period of increased success. Their increased success has led them to need a Customer Relationship Management (CRM) solution. Businesses must typically pay attention to how they engage with customers and invest more resources in IT and CRM E-commerce. To deliver far higher customer satisfaction, they need to become conscious and be able to read their customers’ minds and understand their spending habits and needs (Ngangi, 2019). They should also establish a customer-focused culture in their organizations or businesses. To have a mutual relationship with the customer, worthy and cognizant managers should be hired, and sufficient funds set aside.

As a result of their study, executives have narrowed the selection of the CRM solution down to three potential options:

* A Commercial off-the-shelf solution.
* An Open-Source Solution.
* An in-house solution built by a student.

**Scope of the Risk Assessment**

ACME Manufacturing is an SME (Small/Medium Enterprise) employing 150 staff.

The external (customer) interface is a web page collection that allows users to enter data and get information from the program. Initially, the enterprise allowed the management staff to track their transactions via spreadsheets and constantly update their records manually. Therefore, the scope of this assessment seeks to analyze and assess the credibility of embracing the implementation of customer relationship management systems that would see the enterprise thrive in all its diverse processes.

**Literature Review of Existing Organizations**

The figure below includes a comparison of other manufacturing companies that are of a similar size to ACME, who have successfully implemented a CRM solution and how they have benefited from it.

|  |  |  |  |
| --- | --- | --- | --- |
| **Manufacturing Company** | **Number of Employees** | **Yearly Income** | **Improvements from CRM Implementation** |
| Kayserberg | 116 | £ 340 Million | * Increased overall sales. * Easier to target sales to specific areas. * Improved overall marketing strategies. |
| SOMEFLU | 50 | £ 9 Million | * Increased sales efficiency. * Better project management. |
| O'Neal Steel | 200 | £ 682 Million | * Improved overall sales * Simplification of storing customer information * Better resource usage planning. * Detailed overview of data to use for rival company comparisons. |

Figure 1. (Hasan et al, 2015; Dun & Bradstreet, 2022; DS Smith Plc, 2008)

**Risk Assessment Approach**

The different technical and business risks that are likely to be incurred in each solution can be presented as follows:

|  |  |  |
| --- | --- | --- |
| **ERP System** | **Technical Risks** | **Business Risks** |
| **COTS Solution** | * The significant learning curve for upkeep and implementation. * Specific hardware requirements to implement. * Using closed source code or proprietary code. * Pre-packaged, with no access to review source code or architecture. * Lack of updates over time. * Difficult to verify the Security of COTS. * The vendor may pull the plug on the support. * COTS software is generally a more attractive attack target than custom code. * Easy access for attackers as COTS are well known publicly. * Options to access solutions are well documented. * “The ability to explore the functionality or dysfunctionality of the code is well documented” (Miller, 2006). * It can be easily experimented on by the black hat community. * Easy to reverse engineer. * “Information is shared among the black hat community on vulnerabilities, viable attack patterns, and the code to implement attacks” (Miller, 2006). * Unable to verify the quality of code that is written. * None or little publication on coding practices related to security. * The skills and experience required to test solutions may be outside the business's budget. * Connectivity to external services and data stores may open doors to external unauthorized access (Lesser et al, 2020: 63). * Code may not be tuned to the specific security requirements of the business (Miller, 2006. * The introduction of the COTS solution may open up new vulnerabilities for hackers to enter the network. * The introduction of cots may provide a point of entry for Invasion of Privacy Attacks. * The introduction of cots may facilitate Denial-of-Service Attacks. | * Significant Initial Cost and Upkeep. * Need to train staff members on the software. * Software may not be ideal for the company in the long run. * Lack of feature request processes * Lack of product enhancements * Paying for features that may not be needed. * Compatibility issues which may lead to operational issues. * Software vendors have very limited liability in the event of a failure of their code or breach as a result of flaws in their product (Linh et al, 2019: 180). * Software is written for general use and may not be compatible within the business environment (Miller, 2006). |
| Open-Source Solution | * Specific hardware requirements to implement. * Software may not be compatible with current hardware. * Security of the software. * Source code is available publicly, so vulnerabilities are frequently reported. * Vulnerabilities and exploit techniques are well known and documented. * Multiple available unsupported software versions. * Code is easy to reverse engineer and manipulate. * Non-availability of security updates. * Code failure may be difficult to fix. * The presence of zero-day or unknown vulnerabilities, which may be already exploited by the progressive black hat community (Duan, 2019). * Possible availability of backdoors. | * No enterprise-level support outside of forums. * Possibility of software being discontinued. * Possible security vulnerabilities. * Inconsistent software updates (Sherlock et al., 2018). * No formal software license. |
| In-House Solution | * The leading development is done by a student, leading to less than ideal security and optimization. * Specific hardware requirements to implement. * Need for regular software updates and maintenance. * A student may not be familiar with the Secure SDLC process, leading to non- sanitized code. * Code failure may significantly impact the business as the student may lack contextual business information when developing the solution (Dissanayake, 2019). * Lack of maintenance if students leave the business. * Lack of regular updates and testing due to limited or no resources. * Introduction of security issues into the business environment. | * Significant delay in software implementation due to waiting for development (Devadiga, 2018). * May need to spend extra money hiring more developers and support staff. * No external enterprise-level support. * Development and maintenance costs. |

Figure 2. Risks associated with ERP systems

**Business Risks to be overcome**

In the quest for the implementation of a CRM solution, ACME has several potential business risks that it must first overcome. A case in point is the use of the wrong CRM software. While choosing a system to use, an enterprise must overcome falling into the trap of choosing the inappropriate application. Which may not fit the organization’s objective scale with the business and even may not have the needed features for the particular industry. In addition, the business risks associated with security and privacy issues should be overcome. This means that the CRM system being used must be well equipped with security features to avert potential security threats. In the case of the in-house software chosen by the student, IT professionals as well as other security professionals may need to ascertain that the software in use matches the recommended security standards for operation.

**Disaster Recovery Plan /Solution**

For businesses, a disaster recovery plan is essential in restoring normal operations in case of a disaster. Therefore, enterprises need to follow the appropriate steps to create a relevant and valuable disaster recovery plan (Budiman et al, 2020). For instance, a company should formulate a well-written plan that ascertains that operation is not compromised when an emergency or disaster strikes and test the plan to confirm its eligibility. Finally, an enterprise should ensure the plan is tested regularly to check if it meets the ever-changing environment from new applications, new staff, and overall newer functionalities.

Hence, in this case, when an emergency occurs, the IT department will seek support from the enterprise’s authority to formulate and implement the plan. After that, instruct the planning team for every business component that will subsequently accomplish the risk assessment. Therefore, the team will work to identify critical sources such as systems involved in failures and other potential issues. After which a continuity strategy will be determined for restoring processes. Finally, the plan will be reviewed and implemented accordingly for efficient and productive business processes.

**References**

Barros-Justo, J.L., Pinciroli, F., Matalonga, S. and Martínez-Araujo, N. (2018) What have software reuse benefits been transferred to the industry? A systematic mapping study. Information and Software Technology, 103(1): 1 - 21.DOI: https://doi.org/10.1016/j.infsof.2018.06.003

Budiman, K., Arini, F.Y. and Sugiharti, E. (2020) Disaster recovery planning with distributed replicated block device in synchronized API systems. Journal of Physics: Conference Series.1567(3): 1 – 7. DOI: 10.1088/1742-6596/1567/3/032023

Devadiga, N. (2018) A case study on software requirements engineering using the FBI virtual case file project report. International Journal of Advanced Engineering Research and Science. 5(4): 7 – 9. DOI: 10.22161/ijaers.5.4.2

Dissanayake, G. (2019) A Comparison of Security Risk Analysis in the In-house IT Infrastructure and Cloud Infrastructure for the Payment Gateway System. Avaliable from: https://www.semanticscholar.org/paper/A-Comparison-of-Security-Risk-Analysis-in-the-IT-Dissanayake/2a0f65e4269f2617f95a844231f49f604f4b2ee4 [Accessed 16 March 2022].

Duan, R. (2019). Toward solving the security risks of open-source software use. Avaliable from: https://cyfi.ece.gatech.edu/publications/DUAN-DISSERTATION-2019.pdf [Accessed 16 March 2022].

Dun & Bradstreet. (2022) O'Neal Steel, LLC. Available from: https://www.dnb.com/business-directory/company-profiles.oneal\_steel\_llc.f03187793f53c09973e1bff7f69aa351.html [Accessed 15 March 2022].

Dun & Bradstreet. (2022) SOMEFLU. Available from: https://www.dnb.com/business- directory/company-profiles.someflu.99d1d7bbddc2c872051d46bef4134cc8.html [Accessed 15 March 2022].

DS Smith Plc. (2008) Delivering Substantial Progress: Annual Report 2008. Available from: https://www.annualreports.com/HostedData/AnnualReportArchive/d/LSE\_SMDS\_2008.pdf [Accessed 15 March 2022].

Hasan, N., Salamon, H., Zulkeply, M., Dahlan, H., Hussin, Ab. (2015) Review of CRM Implementation Based on Three Companies in Manufacturing Industry. Journal of Information Systems Research and Innovation. 9(2): 43-48. Available from: https://seminar.utmspace.edu.my/jisri/download/V%209-%202/JISRI-Paper6.pdf

Lesser, D., Katra, I., Dorman, M., Harari, H., Kloog, I. (2020) Validating and Comparing Highly Resolved Commercial "Off the Shelf" PM Monitoring Sensors with Satellite-Based Hybrid Models for Improved Environmental Exposure Assessment. Sensors 21(1): 63. DOI: https://doi.org/10.3390/s21010063

Linh, N.D., Hung, P.D., Diep, V.T. and Tung, T.D. (2019) February. ‘Risk management in projects based on open-source software’. Proceedings of the 2019 8th International Conference on Software and Computer Applications. Penang, Malaysia. 19-21 February. New York, United States: Association for Computing Machinery.

Miller, C. (2006) Security Considerations in Managing COTS Software. Avaliable from: https://www.cisa.gov/uscert/bsi/articles/best-practices/legacy-systems/security-considerations-in-managing-cots-software [Accessed 22 March 2022].

Ngangi, S.C.W. & Santoso, A.J. (2019) Customer acceptance analysis of customer relationship management (CRM) systems in an automotive company using Technology Acceptance Model (TAM) 2. Indonesian Journal of Information Systems 1(2): 133 -146. DOI: 10.24002/ijis.v1i2.1993

Sherlock, J., Muniswamaiah, M., Clarke, L., and Cicoria, S. (2018) Open Source Software Opportunities and Risks. Available from: https://arxiv.org/abs/1812.11697 [Accessed 14 March 2022].

Sourizaei, M., Keikhayfarzaneh, A., Khalatbari, J., Keikhayfarzaneh, M. (2011) Customer Relationship Management (CRM) and Its Risk Factors. International Journal of Scientific & Engineering Research. 2(8): 1-3. Available from: https://www.ijser.org/researchpaper/Customer\_Relationship\_Management\_(CRM)\_and\_Its\_Risk\_Factors.pdf