

CSEC 733.01

Final Team Project

Risky Business

Duncan Brickner , Sergei Chuprov , Pranav Sarma Venkatramanan



Consulting Services for Vague Inc.

4/6/22

Consulting Services Report for Vague Inc.

Table of Contents

Summary	3
Overall Assessment	3
Business Impact Analysis	3
Vulnerabilities Identified and Recommendations:	4-5
PCI-DSS Compliance	5
Other Findings	5-6
Appendix 1: Business Impact Analysis	6-7
Appendix 2: Risk Matrix	7-8
Description of likelihood categories:	7
Description of likelihood categories:	7
Risk Matrix:	8
Appendix 3: Monte Carlo	9
Appendix 4: Team Collaboration	9-10

Summary

In this report, we provide the comprehensive risk analysis and evaluation for the Vague Inc. We analyzed the internal and external information about the company, and conducted interviews with the employees of three company's departments: Core Business, HR, and IT. We used the provided information to perform Business Impact Analysis for each of these departments. In addition, based on the provided information, we determined potential risks and their likelihood, impact levels, and company's risk appetite.

Overall Assessment

Provide an opinion about the state of the company's controls evaluated.
We have found 5 vulnerabilities with the following ratings:

- 3 High risk
- 1 Significant risk
- 1 Medium

Overall, we believe that your organization is not well positioned to address cyber risks and we recommend your organization to address the mitigation of the critical vulnerabilities identified as soon as possible.

Business Impact Analysis

We conducted Business Impact Analysis for the three Vague Inc major departments: Core Business, IT, and HR. The Business Impact Analysis included departments' persons in charge interviews and follow-up questions based on the information provided by the employees. According to the analysis results, we have come to the following conclusions.

First, the most important process in the company is identified as software development. The product the company develops and sells makes the major part of their revenue. The company has 667 employees and can be classified as medium-size.

The company is based in New York State and provides services and products to the US and EU customers. Working with EU clients makes the company required to comply with GDPR, however, this regulation was not mentioned by the company's employees when we asked: "Are there any policies you have to comply with (GLBA, HIPAA, etc.)?" in our follow-up questions.

Second, the company actively relies on 3rd party solutions and services, such as AWS for data storage and Salesforce for CRM purposes. However, the company's employees state that they do not have any contingency plans for 3rd party vendors in place. This fact makes the company vulnerable to any kind of service interruption by the 3rd parties. For example, if all the information will be lost or damaged, the company needs a clear plan of actions on how to recover with minimal losses.

Moreover, the company does not have a DLP-system in place, which makes its internal information vulnerable for potential leakage out of the security perimeter.

Vulnerabilities Identified and Recommendations:

We have identified and reviewed your organization's critical processes and have classified the following list of vulnerabilities. Risk rating and recommendations for improvement have been provided.

Vulnerability Name: Smartphone compromise

Vulnerability Description: Attackers are increasingly stealing or hacking smartphones in order to bypass two-factor authentication. No controls are evident for this issue.

Risk Rating: Not Likely * Moderate = **Medium Risk**

Recommendation: Move from two-factor authentication to multi-factor, or have the second factor be something other than a texted code. Provide employees with smartphones or have a corporate policy to help protect personal devices.

Vulnerability Name: Data compromise

Vulnerability Description: While the facility has extensive measures in place for removing malicious employees, some measures to detect them in the first place are absent. In particular is a lack of file integrity software, that would prevent employees from modifying important files maliciously.

Risk Rating: Implausible * Moderate = **Significant Risk**

Recommendation: Obtain appropriate file integrity software. It may also be possible to mitigate this issue with existing software if appropriately used. For example, network monitoring, ACLs, & access control logs could be configured to address most forms of this issue.

Vulnerability Name: There are no contingencies in place for 3rd party failures (both physical & technical)

Vulnerability Description: The company actively uses services provided by 3rd parties, such as AWS cloud for data storage. In the BIA questionnaire, one of the company's employees responded to the question 1.3: "... As well as our AWS cloud storage that holds a lot of personal information". Any AWS failure in providing the service will lead to data availability violation. Also, data stored in AWS can be maliciously or unintentionally modified or leaked, which violates its integrity and confidentiality. No contingencies in these scenarios might lead to catastrophic consequences for the company.

Risk Rating: Not likely * Extreme = **High Risk**

Recommendation: To create a working group (consisting of CEO and persons critical to departments operations) and develop contingency plans for various potential scenarios. The process is not expensive, but the possible outcomes can save the company in case of disaster.

Vulnerability Name: Physical Impersonation

Vulnerability Description: In the company's network structure, it is stated that the badge-based automated access is employed as a physical security measure to avoid the situation when a stranger can get inside the company's office. However, if the system is 'automated', such a badge will allow the outside person to get inside the company's office and get unauthorized access to the confidential information in case of the badge loss or theft. In addition, such a person can maliciously modify or destroy the information, and can cause physical damage to the company's equipment or employees.

Risk Rating: Probable * Extreme = **High Risk**

Recommendation: Add multi-factor authorization on the physical access point (e.g. fingerprint or face recognition for the employees). Such a measure would require much more effort from the attacker and decrease the chance of the impersonation.

Vulnerability Name: Internal information Leakage

Vulnerability Description: According to the documents and information, provided to us by the company, there are no DLP-systems in use. This fact automatically creates a number of vulnerabilities related to the information leakage. A DLP-system allows the company to monitor all the access and flow of information inside company devices and network, and allows it to identify cases of information misuse and negligence by the employees. For example, it can detect and prevent cases of unauthorized copying of the information or sending it to private email addresses.

Risk Rating: Very Likely * High = **High Risk**

Recommendation: To install a DLP-system. There are a lot of solutions on the market.

Vulnerability Name: Add Name

Vulnerability Description: Provide details

Risk Rating: based on risk matrix

Recommendation: Describe recommendation

PCI-DSS Compliance

We have reviewed the provided PCI-DSS self-questionnaire and have determined that

Your organization is not in compliance due to: Requirement 11 (Regularly test security systems and processes). While some vulnerability scans and intrusion detection are done, certain other network scans and penetration tests are not.


We recommend the following to bring your organization to compliance:

Add policies requiring the missing evaluations, and establish processes for ensuring they are performed on a regular basis (at least quarterly).

Other Findings

In the course of our evaluations, we have discovered that an ex-employee accessed your network with malicious intent. We have performed an evaluation of risks and costs associated with this event happening again. Results can be found in Appendix 3. The vulnerabilities and

financial costs used to perform the Monte Carlo analysis can be found here:

 **Monte Carlo Event** . Due to the high revenue your company produces, we selected rather high values for potential damage. As such, the overall estimated cost of this incident is quite high.

The risk appetite your organization has established for this event is not appropriate. We provide the following recommendations:

- 1) As possible, increase your risk tolerance by budgeting some additional funds for incidents
- 2) Implement controls to mitigate the identified vulnerabilities. While this may not be possible for vulnerabilities like AWS server compromise, issues like back doors & record compromise can be mitigated with DLP, access controls, & data integrity / file monitoring software
- 3) Continue, and improve as possible, your employee vetting process, as well as procedures for terminating problematic employees

Appendix 1: Business Impact Analysis

Below we provide the links to our BIA questionnaires for the three Vague Inc. departments, and to the follow-up questions, formulated based on the BIA questionnaire responses:

[Core Business](#)

[HR](#)

[IT](#)

[Follow-up Questions](#)

Department Name	Process Name	Systems	Resources	Criticality Rating	RTO (RPO)
Physical Security	Video Surveillance	Video surveillance software	Cameras, Security Officer	High	4 hours
Core Business	Software Development	Microsoft Office 365, Iron Mountain	Employess, Laptops, Routers, Switches, Servers, and Access Points	High	3 weeks
HR	Hiring employees	SalesForce, Microsoft Office 365, AWS	Employees, Laptops, Printers, Scanners	High	3 months (\$0)
HR	Paying employees	SalesForce, Microsoft	Employees, Laptops,	Medium	1 week (\$222,000)

		Office 365, AWS	Printers, Scanners		
IT	Vulnerability Assessment	Vague Defense	Employees, Workstations, Laptops, Printers, Servers	High	\$2,000,000
IT	Network Infrastructure Maintenance	Servers, server room, workstations, proprietary software, CMS, Customer records, client data and related files	Employees, Workstations, Laptops, Printers, Servers	High	\$5,000,000

Appendix 2: Risk Matrix

Description of likelihood categories:

Likelihood	
Implausible	10%
Not likely	25%
Probable	50%
Very Likely	75%
Definite	90%

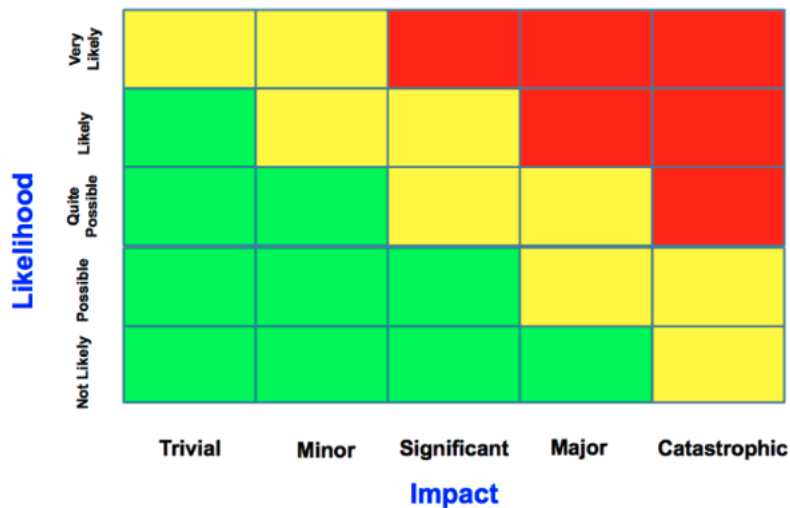
Description of likelihood categories:

Impact	
Minimal	Insignificant financial (<10K), time (<1hr), or reputational impact
Low	Low financial (~100K), time (~1day), or reputational impact
Moderate	Moderate financial (1M+), time (5day+), or reputational impact
High	High financial (>\$50M, but <\$100M), and reputational impact, down-time (>2 weeks, but <1 month)
Extreme	Significant cost (>\$100M), down-time (>1 month) or loss of reputation

Risk Matrix:

Impact	Minimal	Low	Moderate	High	Extreme
Likelihood					
Implausible	Mild	Mild	Significant	Significant	Medium
Not likely	Mild	Significant	Medium	Medium	High
Probable	Significant	Medium	Medium	Medium	High
Very Likely	Significant	Medium	Medium	High	Critical
Definite	Medium	High	High	Critical	Critical

Example:



Appendix 3: Monte Carlo Simulation

Below we provide the screenshot with the results obtained using the Monte Carlo simulation.

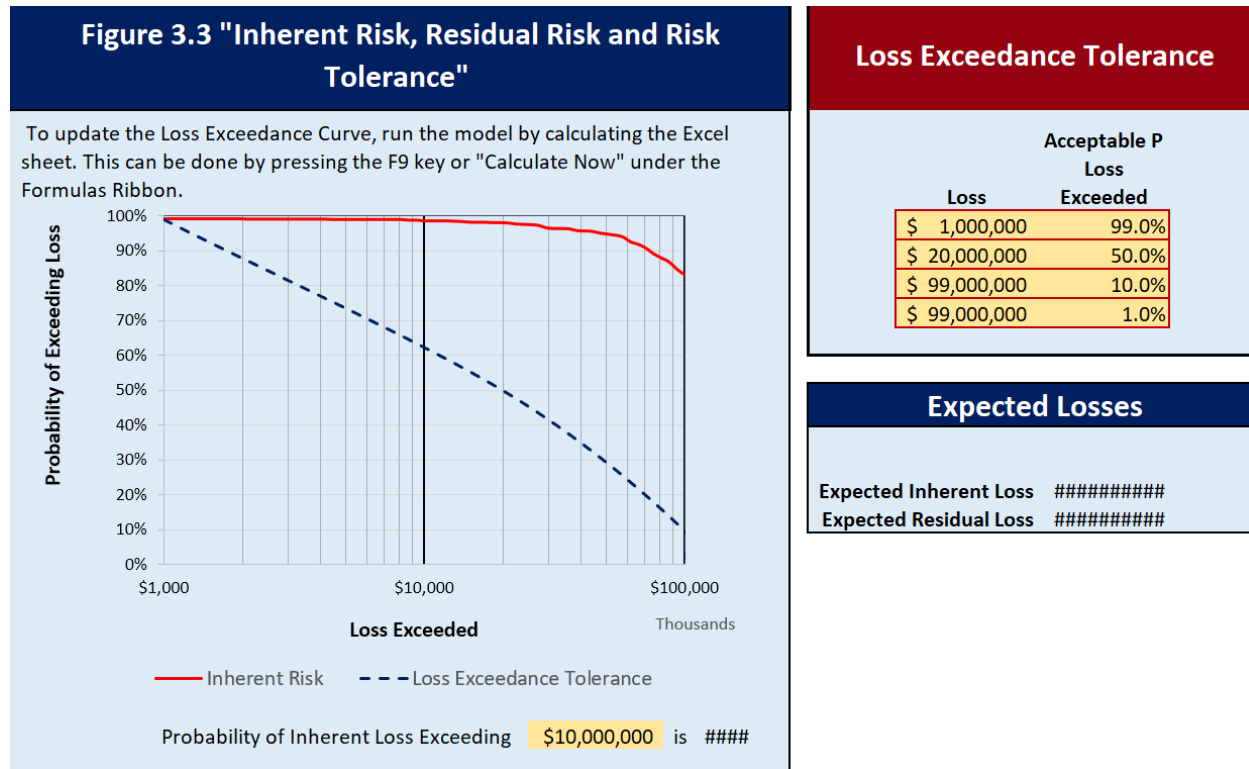


Figure 1. Monte Carlo simulation results

Appendix 4: Team Collaboration

Team Collaboration details:

Report Sections	Team Member Responsible	Division Of Work
		<ul style="list-style-type: none"> Team members participated equally Member X developed this document alone (or with little input from the team) Member X and Y developed this document (with assistance from Z)
PCI-DSS Compliance	Duncan Brickner	Developed this document with minimal input from the team
Appendix 2	Duncan Brickner & Sergei Chuprov	Developed this document together
Appendix 3	Sergei Chuprov	Developed this document with moderate input from the team
Appendix 1	Sergei Chuprov	Developed this document with some input from the team
Other Findings	Duncan Brickner	Developed this document independently

Summary	Sergei Chuprov	Developed this document independently
Business Impact Analysis	Sergei Chuprov	Developed this document with some input from the team
Overall assessment	Pranav Sarma	Developed this document with input from the team
Presentation Sections	Team Member Responsible	Division Of Work
		<ul style="list-style-type: none"> ○ Team members participated equally ○ Member X developed this document alone (or with little input from the team) ○ Member X and Y developed this document (with assistance from Z)
BIA	Sergei Chuprov, Pranav Sarma	Team members participated equally
Vulnerabilities	Sergei Chuprov, Duncan Brickner, Pranav Sarma	Team members participated equally
PCI-DSS Compliance	Duncan Brickner	Developed this document alone
Monte Carlo	Pranav Sarma	Developed this document alone