RISK ASSESSMENT REPORT

FOR VAGUE INC.

PREPARED BY:

DUNCAN BRICKNER
SERGEI CHUPROV
PRANAV SARMA V

CONTENTS:

ABOUT THE COMPANY

Company Name: Vague Incorporated

Industry: Company sells cybersecurity services related to health care and private health information

Size: Medium
Number of Employees: 667
Annual Revenue: $200 million
$299,850.00 per employee

Location:
Based in New York State
Sells to customers across the United States and in the EU.

Business Impact Analysis. Core Business

Summary:

- **Employees:** 222
- **Location:** 2nd floor global headquarters in New York
- **Main critical business applications/software:** Microsoft Office 365, Iron Mountain for our backup solution

Business Process	Timing/Duration	Operation Impacts	Financial Impacts
Software Development	>1 week This would have a greater impact at the end of a quarter or before a major patch.	Potential missed cyber attacks/compromises	$2,000,000

Points of Contact	Name and Title	Critical to Completing the Process (Yes, No / Subject Matter Expert)
Leader	Jess Beckwith	No
Backup Leader	Craig Gebo	No
Team Members (Repeat row as needed)	Nick Graca	In charge of Core Business
Team Members (Repeat row as needed)	Gaurav Sharma	No

Asset	Impact Level
Software	High
Backup Storage	Moderate

Priority	System Resource/Component	Maximum Tolerable Downtime
1	Software Development	3 weeks

Business Impact Analysis. HR

Summary:

- **Employees:** 222
- **Location:** 1st floor global headquarters in New York
- **Main critical business applications/software:** The employees themselves, SalesForce application, employee database (stored in AWS)

Business Process	Timing/Duration	Operation Impacts	Financial Impacts
Hiring employees	Timing: end of quarter. Duration: > 1 year	Lower than expected workforce to cover all responsibilities.	$222,000
Paying employees	Timing: end of week / pay period Duration: > 2 weeks	Lower morale, loss of employee loyalty, increased turnover.	$0 (pay employees back equal to what they were not paid, no interest)

Points of Contact	Name and Title	Critical to Completing the Process (Yes, No / Subject Matter Expert)
Leader	Jess Beckwith	No
Backup Leader	Craig Gebo	In charge of HR
Team Members (Repeat row as needed)	Nick Graca	No
	Gaurav Sharma	No

Asset	Impact Level
Employees	High
SalesForce	Moderate
Employee Database (AWS)	High

Priority	System Resource/Component	Maximum Tolerable Downtime
1	Pay employees	1 week
2	Hire employees	3 months

Business Impact Analysis. IT (1/2)

Summary:

- **Employees:** 222
- **Location:** 4th floor global headquarters in New York
- **Main critical business applications/software:** Vague Defense

Business Process	Timing/Duration	Operation Impacts	Financial Impacts
Vulnerability Assessment	>24 hrs. <72 hrs.	• Risk of zero day exploits • Increased risk of compromise due to unknown vulnerabilities	• Approx. $2,000,000
Network Infrastructure Maintenance	> 24 hrs.	• Delay executing business plan or strategic initiative • May result in loss of network infrastructure and resources	• Approx. $5,000,000

Points of Contact	Name and Title	Critical to Completing the Process (Yes, No / Subject Matter Expert)
Leader	Jess Beckwith	No
Backup Leader	Craig Gebo	No
Team Members (Repeat row as needed)	Nick Graca	No
Team Members	Gaurav Sharma	In charge of IT

Asset	Impact Level
IT Staff	High
Servers	High
Network	High
Workstations	High
Employee Laptops	Moderate
CMS	High
SIEM	Moderate

Business Impact Analysis. IT (2/2)

Priority	System Resource/Component	Maximum Tolerable Downtime
1	Vulnerability Assessment	< 24 hrs
2	Network Infrastructure Maintenance	< 24 hrs

Back-up types	Backup Schedule/Frequency(s)
Cloud	Every day

Hardware name	Hardware type	Description
Cisco Routers	Wired routers	Provides high availability, comprehensive security, integrated wireless, ease of management, and advanced Quality of Service (QoS)
Cisco Switches	Switch	Used to store the arrived packets, process it and forwards it to the specified destination. Cisco switches boast of less costs, more secure and easily scalable network
Networking Cables	Cables	Used to connect one network device to other network devices or to connect two or more computers to share printers, scanners etc
External Hard Drives	Hard drive	Its a component that stores digital content

Vulnerability Risk Table

Impact Likelihood	Minimal	Low	Moderate	High	Extreme
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

Discovered Vulnerabilities

1. **There are no contingencies in place for 3rd party failures (both physical & technical)**

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.

2. **Physical Impersonation**

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.

Discovered Vulnerabilities 2

3. Smartphone compromise

Risk Rating: Not Likely * Moderate = Medium Risk
Recommendation: (i) Upgrade from two-factor authentication to multi-factor. (ii) Use secure physical device for authentication. (iii) BYOD Policy or other system for securing employee devices

4. Data compromise

Risk Rating: Implausible * Moderate = Significant Risk
Recommendation: (i) Obtain appropriate file integrity software. (ii) Configure existing tools to help identify & prevent file modification.

5. Internal information Leakage

Risk Rating: Very Likely * High = High Risk
Recommendation: To install a DLP-system. There are a lot of solutions on the market.

Monte Carlo Simulation

Event:
A disgruntled employee has: ***(i)*** Downloaded a file containing customer personal records and ***(ii)*** Opened a backdoor to access core services

Time: 1 year

Loss exceedance histogram:

RISKS	PROBABILITY	LOSS RANGE
Illegal distribution of the consumers' PII	80%	10M - 100M
Gaining access to the company's confidential data via backdoor	70%	150M - 250M
Damage to the company's reputation due to data leak	50%	50M - 200M
Falsification of records	50%	1M - 10M
Undermining of software/hardware integrity	25%	10M - 100M
Extortion for safe return/deletion of records	10%	1M - 10M
Halting of assembly line operations	5%	40M-80M
Compromise/Destruction of AWS system	1%	100M - 500M
Compromise/Destruction of DMZ Server	1%	100M - 500M

Risk tolerance histogram in order of ***% acceptable loss : cost of loss*** -

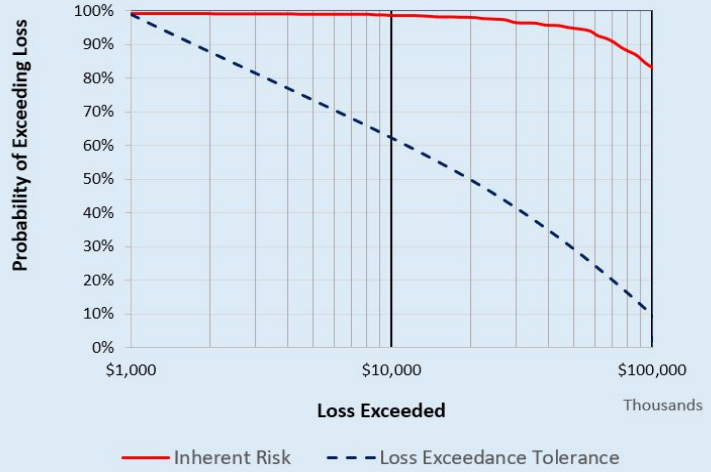
99%: $1M
50%: $20M
10%: $100M
1%: $150M

Monte Carlo Simulation 2

Loss expectancy curve:

Figure 3.3 "Inherent Risk, Residual Risk and Risk Tolerance"

To update the Loss Exceedance Curve, run the model by calculating the Excel sheet. This can be done by pressing the F9 key or "Calculate Now" under the Formulas Ribbon.



Probability of Inherent Loss Exceeding $10,000,000 is ####

Loss Exceedance Tolerance

Loss	Acceptable P Loss Exceeded
$ 1,000,000	99.0%
$ 20,000,000	50.0%
$ 99,000,000	10.0%
$ 99,000,000	1.0%

Expected Losses

Expected Inherent Loss	##########
Expected Residual Loss	##########

PCI-DSS Compliance

Issue: Requirement 11

Regularly test security systems and processes:

In-house application are subjected to vulnerability tests, but there are no more thorough examinations of other parts of the network are done, like penetration tests or attack simulations

This leaves Vague Inc potentially vulnerable from having insecure or unpatched issues hiding in their network

For remediation, we recommend creating a complete policy for security testing, and following through on those requirements (ideally quarterly)

Other Highlights

Small issue: Certain policies, such as an overarching security policy & one for use of third-party applications that ship with defaults, exist within the company but were not recorded among controls. These had to be confirmed verbally.

Good Note: Company has excellent firewalls, strong use of encryption, & thorough physical security controls

THANK YOU FOR YOUR TIME!