MEMORANDUM

TO:	Dr. Babik, Assistant Professor, James Madison University
FROM:	Trevor Hudson, Jared [redacted]
DATE:	4/18/2023
SUBJECT:	Risk Assessment and Risk Mitigation Strategy for WoodBlock LLC

PURPOSE

Our potential investor is gauging his interest in our company and wants us to identify and assess all potential risks and vulnerabilities pertaining to availability of the ecommerce site and compromised confidentiality of sensitive customer data. To identify these vulnerabilities and risks, we examine all possible asset-threat-impact scenarios and quantify them to better understand the mitigation strategies needed for improved security of our assets.

PROBLEM

Vulnerabilities are the gateway to exposure which can be detrimental to our operations and could result in loss of critical data or even lawsuits from our customers. To prevent this, we need to stay updated and informed on all possible vulnerabilities to limit our risk or at the very least be able to mitigate the impacts of our risks by performing risk analysis.

ANALYSIS

Our assets are identified by all devices and information used in everyday business operations from the physical hardware to the electrical service used to run all devices. Threat identification was made based off our potential investor's worries of SaaS outage and compromised confidentiality of sensitive customer data such as credit card information. Those assets necessary to do business were given high levels of risk when accompanied by highly vulnerable threats. Each of the threat scenarios in the risk analysis were given the highest risk score due to the importance of those mission-critical assets with threats of the highest vulnerabilities, if any of those scenarios played out, they would have crippling effects on the business and/or our customers. Such effects would make the ecommerce site unusable for an unknown amount of time or potentially have our customer's credit card information leaked to the world. It is assumed that both house's routers contain a switch and a modem so those are lumped into one asset, meanwhile each house has a separate WAP to handle the smartphones.

CONCLUSION / RECOMMENDATIONS

Following our informal, formal, and technical controls in table 5 will allow us to mitigate these potential risks as best as we can and ensure the protection of our customer's data and limit our website's downtime. Refusal to follow these procedures could have adverse effects on the company and potentially making us liable for the loss of our customers personal information, which would effectively put us out of business and drown us with legal fees.

Table 1 – Information Assets of WoodBlock LLC

Asset	Asset Category	Asset Type	Asset Importance
Shopify account	Mission-critical SaaS	SS	High (3)
Shopify credentials	Credentials	DB	High (3)
Transactional database	Mission-critical data in cloud	DB	High (3)
Dell laptops (2)	Mission-critical client equipment	HW	High (3)
Samsung Galaxy smartphones (2)	Mission-critical client equipment	HW	High (3)
Other peripheral devices	Peripheral equipment	HW	Low (1)
Inkjet printers (2)	Peripheral equipment	HW	Low (1)
Internet services	Communication services	SS	High (3)
Router and modem (2)	Networking equipment	HW	Medium (2)
WAP (2)	Networking equipment	HW	Medium (2)
Electrical power service	Utility services	SS	High (3)
Web Store front-end information	Important data in the cloud	DB	Medium (2)
Various email/messaging data	Important data in the cloud	DB	Medium (2)
Various files stored on smartphones and laptops	Miscellaneous data stored locally	DB	Low (1)

Table 2 – Threats to Information Assets of WoodBlock LLC

Threat	Threat Category	Threat Type	Primary Impact
Service interruption due to provider outage	Service interruption	DDD	A
Service interruption due to license expiration	Service interruption	DDD	A
Unauthorized access/copying of data with potential disclosure by an outsider	Unauthorized access or disclosure	Intr	C
Unauthorized (intentional or unintentional) disclosure of confidential data by insider	Unauthorized access or disclosure	Intr	C
Device failure or malfunction	Equipment failure	DDD	I
Unintentional breaking of equipment	Human error or unintentional damage	DDD	I
Unintentional alteration or deletion of data	Human error or unintentional damage	DDD	I
Theft of equipment	Intentional removal of tangible property	Intr	A
Intentional breaking of equipment/vandalism	Intentional damage	Intr	I
Intentional alteration or vandalizing of data	Intentional damage	Intr	I
Virus infection or attack	Malware (targeting I)	Intr	I
Ransomware	Intentional removal or obstruction of access to data	Intr	A

Table 3 – High-level Qualitative Mapping of Information Assets, Threats, and Risks for WoodBlock LLC

				Asset Categories in the Relative Order of Importance									
			Asset Categ	1	2	3	4	5	6	7	8	9	10
				Mission-critical data in cloud	*Credentials*	*Mission-critical client equipment*	*Mission-critical SaaS*	*Communication Services*	*Utility Services*	*Important data in the cloud*	*Networking Equipment*	*Miscellaneous data stored locally*	*Peripheral equipment*
Threat Categories in the Relative Order of Vulnerability	**Threat Category**		**Type**	DB	DB	HW	SS	SS	SS	DB	HW	DB	HW
	1	*Unauthorized access or disclosure*	Intr	C/H	C/H					C/L			
	2	*Equipment failure*	DDD			I/H					I/M	A/L	I/L
	3	*Service interruption*	DDD	A/H			A/H	A/M	A/M	A/M			
	4	*Intentional damage*	Intr	I/H		I/H				I/M	I/M	I/L	I/L
	5	*Intentional removal or obstruction of access to data*	Intr	A/H		A/H				A/M	A/L	A/L	A/L
	6	*Malware (targeting I)*	Intr	I/H						I/L		I/L	
	7	*Intentional removal of tangible property*	Intr			A/M					A/L	A/L	A/L
	8	*Human error or unintentional damage*	DDD	I/M		I/M				I/L	I/L	I/L	I/L

Table 4 – Low-level Quantitative Risk Analysis for WoodBlock LLC

Asset	Asset Category	Asset Type (HW, SW, DB, SS)	Asset Importance (H=3 M=2 L=1)	Threat	Threat Category	Threat Type (DDD, Intr)	Primary Impact on C, I, or A	Threat Impact (H=3 M=2 L=1)	Vulnerability (H=3 M=2 L=1)	Exposure Level	Risk Score
Shopify account	Mission-critical SaaS	SS	3	Service interruption due to provider outage	Service interruption	DDD	A	3	3	9	27
Shopify account	Mission-critical SaaS	SS	3	Service interruption due to license expiration	Service interruption	DDD	A	3	3	9	27
Transactional database	Mission-critical data in cloud	DB	3	Service interruption due to provider outage	Service interruption	DDD	A	3	3	9	27
Transactional database	Mission-critical data in cloud	DB	3	Service interruption due to license expiration	Service interruption	DDD	A	3	3	9	27
Transactional database	Mission-critical data in cloud	DB	3	Unauthorized (intentional or unintentional) disclosure of confidential data by insider	Unauthorized access or disclosure	Intr	C	3	3	9	27
Transactional database	Mission-critical data in cloud	DB	3	Unauthorized access/copying of data with potential disclosure by an outsider	Unauthorized access or disclosure	Intr	C	3	3	9	27

Table 5 – Risk Mitigation Strategy Outline for compromised confidentiality of sensitive customer data in the transactional database

Controls	Technical	Formal	Informal
Preventive	Require special authorization to access sensitive customer data. Change credentials at regular intervals. Utilize dual authentication to add an extra layer of security when accessing sensitive data.	Rules against the sharing of customer data and limitations of who has access to such data.	Acknowledgement amongst owners that stresses the importance of protection of sensitive customer data.
Detective	Utilize dual authentication which monitors suspicious attempts to access data.	Laws preventing companies from accessing customer credit card information without consent (regarding the detection of a data breach).	Understanding of personnel to know what to look for to identify a data breach.
Corrective	Notify victimized customers and block IPs of the culprits. Turn off all access to sensitive data to prevent further leaked sensitive data and more unhappy customers.	Rules in place detailing the process of data recovery, disallowing access to data, and notification of those affected.	Understanding the proper course-of-action to take when a data breach occurs.