Assets	Vulnerability	Threat	Risk and Potential Impact	Solution
Customer Data, Financial Data	Weak Encryption and outdated systems	Hackers using brute-force attacks or stolen credentials	Data breach which leads to loss of reputation and potential financial penalties from customers **High**	Strong implementation of encryption, regular system updates, and employee training about data security
Confidential Information	Human error	Employees	Accidental disclosure of information results in reputational damage, a loss of trust from customers, and account takeover **High**	Implementation of security awareness training and practicing data minimization methods
Information Sharing	Lack of communication protocols, data stored in isolated systems	Internal Miscommunication	Department silos results in reputational damage and end of customer trust **Medium**	Implementation of set information sharing protocols and breaking down departmental barriers through effective communication
Employee Devices	Unpatched Operating Systems & Applications	Malicious individuals and/or organizations	Data breaches, malware infections result in	Execution of a centralized patch management

		exploiting known vulnerabilities	financial losses and reputational damage. Moreover, a higher chance at vulnerability for remote laptops is emphasized because of less controlled environments. **High**	system for prompt OS and application updates.
Intellectual Property	Unsanctioned cloud storage usage	Unauthorized access or data leaks due to insecure cloud storage services	Loss of competitive advantage and potential copyright infringement lawsuits. **High**	Development and enforcement of a cloud storage policy which allows approved and secure cloud services to be implemented within departments. Furthermore, education for employees about the risks of Shadow IT and providing secure alternatives for collaboration can enhance protection of this asset.
Company Website	Outdated Content Management System (CMS) vulnerabilities	Malicious individuals and/or organizations	Website downtime, potential malware	Application of a a secure and updated CMS. Regularly

		exploiting known vulnerabilities in the CMS to inject malware or deface the website	infections for visitors which underscore possible reputational damage and misinformation. **Medium**	update and patch the CMS to address vulnerabilities.
Network Infrastructure	Misconfiguration, Unpatched Software	Hackers exploiting outdated software and Denial-of-Service Attacks (DDoS)	Network Outages, Data Breaches. Business disruption, revenue loss, reputational damage **High**	Carrying out secure network configuration standards, consistent strict patching schedules, and conducting vulnerability assessments
Software Applications	Unauthorized Access, Software Vulnerabilities	Malicious Actors (Hackers), Software Bugs	System Outages, Data Loss. Business disruption, productivity loss, potential compliance violations **High**	Performing strong access controls, conducting regular software updates, and carefully selecting secure cloud providers with robust security measures for company use.
Company Social Media Accounts	Phishing attacks targeting account credentials	Hackers gaining access to social media accounts for fraudulent activity or brand reputation manipulation	Reputational damage, potential financial losses, loss of control over brand messaging. **Medium**	Enforcement of strong password complexity and authentication methods (i.e. Multi-factor authentication) for social media

				accounts, conducting training for social media managers on phishing attacks, and best practices for account security.
Office Environment	Unlocked computers with sensitive data displayed on screen	Unauthorized access to confidential information by colleagues or visitors	Potential data breaches or accidental data exposure. Low	Employee education about the importance of locking devices when unattended to minimize displaying sensitive information and requiring screen saver timeouts on devices with password protection
Printing Devices	Lack of authentication and encryption for printing jobs	Unauthorized access to sensitive documents sent for printing	Potential data breaches or accidental exposure of confidential information. Low	Network printing authentication implementation for access control when it comes to print jobs within the company. Encryption of print jobs may also be considered for further security.
Incident Response Plan	Lack of a defined plan or	Delayed response and	Increased risk of data	Creation of a thorough

	employee training	increased damage from security incidents	breaches, financial losses, and reputational damage. **Medium**	incident response plan that outlines the different procedures for detection, containment, eradication, and recovery from security incidents. Conducting regular employee training on the incident response plan and how to report suspicious activity should also be considered
Third-Party Vendor Applications	Insecure coding practices by the vendor leading to vulnerabilities	Malicious actors exploiting vulnerabilities in vendor applications to gain access to the company network	Data breaches, malware infections, disruption of critical business processes. **Medium**	Thorough security assessments prior to the integration of third-party applications within the company. Negotiation on contracts with vendors must emphasize the need for strong security clauses and data breach notification requirements.
Data Disposal	Inadequate	Data breaches	Potential data	Secure data

Procedures	data wiping practices	from residual data on decommissioned devices (e.g., hard drives, servers)	breaches of sensitive information on old equipment. **Low**	wiping procedures implementation for all end-of-life devices to ensure complete data removal and considering physical destruction of storage media for highly sensitive data.
Third-Party Investment Custodians	Inadequate security practices by the custodian	Security breaches at the custodian leading to loss of customer assets or disruption of investment transactions	Financial losses for customers, reputational damage, potential lawsuits. **Medium**	Conduct due diligence on the security practices of third-party investment custodians, as well as, negotiation for contracts with strong security clauses and data breach notification requirements.