Project Name	Lemonade CyberSecurity
Project Manager	Sprint Team 02
Date Updated	3/25/2024
Revision	1

Impact					
	5	10	15	20	25
	4	8	12	16	20
	3	6	9	12	15
	2	4	6	8	10
	1	2	3	4	5
	Likelihood				

IMPACT		LIKELIHOOD	
Very Minor	1	1 - 20%	1
Minor	2	21 - 40%	2
Moderate	3	41 - 60%	3
Significant	4	61 - 80%	4
Catastrophic	5	81 - 99%	5

RESPONSE
Avoid
Reduce
Fallback
Transfer
Share
Accept

RISK ID NO.	RISK NAME	RISK DESCRIPTION	RESOURCE IMPACTED	CAUSE	ASSIGNED TO	IMPACT	LIKELIHOOD	SCORE	RESPONSE	PREVENTION MEASURES	START DATE	DUE DATE	STATUS	NOTES
1	Sensitive Data Leak	Bad actors or Crawling Search Engines can access sensitive customer data (PII, PHI, Credit card information) **exploiting the WebApp Vulnerabilities**. Such an attack may lead to - **Legal and Regulatory Compliance issues**. (GDPR/HIPAA/SOC 2 Violations) - damaging Reputation and - damaging future business.	Data Reputation Customer Satisfaction(Trust)	- Web App Vulnerabilities, - Lack of Encryption, - Absence of WAF, - Absence of DLP	CISO	5	4	20	Reduce, Transfer	- Secure Web App Design (OWASP Guidelines etc) - Data Encryption, - Input validations and robots.txt, - **E-discovery and DLP with Redaction**. - WAF, - Automate SOC 2 Compliance monitoring tools - Monitoring with SIEM/SOAR and Threat Modeling - IPS (optionally)				
2	Credentials Compromise	**Phishing email leads, other Social engineering attacks** and **third-party contractors/services** can lead to **Compromised credentials** to various company accounts including slack and Microsoft Office Suite. This can have myraid of adverse consequences, not limited to but including - unauthorized access, - data breaches and - disruptions		- Weak passwords, - unencrypted communications, - compromised endpoint devices, - key-loggers (from malware), - Employees falling victim to social engineering	CISO	4	4	16	Reduce	- MFA, - CASB, - Employee awarenessTraining, - Automate detection/response with EDR, SIEM/UEBA/SOAR - DLP with Redaction (for Data Leak prevention)				
3	Lack of Formal Cybersecurity Governance Model	The **absence** of a structured governance model for cybersecurity operations, including **outdated** or **infrequently reviewed** policies, can lead to - poor security posture - amplified incident impact due to lack of relevant policies and procedures		- poor cybersecurity posture - mismanagement due to lack of plan or direction	CISO	4	4	16	Reduce	- Build a comprehensive **Cybersecurity plan with a framework like NIST 2.0** - **SOC 2 Compliance for Secure storage and process of Client data - annual maintenance effort and costs - need for continuous compliance monitoring** - **ISO/IEC 42001 for AI** (since Lemonade is global) OR NIST AI RMF 1.0 for the AI products in use - Easily accessible Documentation from Asset Management to IR procedures - Centrally managed Governance solutions				
4	Ransomware/Malware Attack	**Phishing email leads, compromised end-points, Document uploads via web or mobile interface** can allow malware to intrude and lead to Ransomware or other Malware attacks in the Lemonade's network. This may lead to - Operational disruptions and - loss of data		- Lack of Awareness, untrained employees - Absence of input-validation, - Absence of WAF, - Unprotected Endpoint devices - Improper/Absent patch-management	CISO	3	4	12	Reduce	- Multiple Backups, - IPS, - SIEM/SOAR - EDR				
5	Lack of centralized Incident Response and Business Continuity	There is an incident response plan for specific events like ransomware, but details about the broader business continuity plan are unknown, suggesting this area needs more development (may not be as critical as direct threats like data breaches). - mismanaged recovery operations - amplified incident impact due to lack of relevant policies and procedures		- poor cybersecurity posture - mismanagement due to lack of plan or direction	CISO	4	3	12	Reduce	- Build a comprehensive IR and BC plan - Easily accessible Documentation - Centrally managed Governance solutions				
6	Cloud Vendor Network Compromised	**Vendor uses unencrypted cloud communication (MIGRATION)** or experiences **Hypervisor attacks**. This may lead to - Operational disruptions and - data leaks		- Miss in SLAs or - Attack on the Cloud - Lack of proper Encryrion - Insecure communications	CISO	4	3	12	Reduce, Share	- Review SLA and shared responsibility clauses & use in #3, - CASB - Encrypt all data in transit, - DLP with redaction				
7	Intellectual Property/Software Theft	Bad actors (competitive sabotage) or disgruntled employees can **exploit vulnerabilities in dev environment/repositories**. Such an attack may lead to - exposed vulnerabilities and - loss to competition due to loss of Intellectual Property		- Lack of Encryption, - Absence of NG-Firewall, - Absence of DLP	CISO	3	3	9	Reduce	- Encryption, - DLP with Redaction, - RBAC				
8	Compromised Third-party AI	If **third-party AI provider Rasa is compromised**, then AI Cooper/Maya/Jim can also be compromised, that can lead to **business logic malfunction** and other process disruptions. If **AI/ML models used for security (that analyze threat feeds) are compromised**, the security operations are compromised. AI used can be subject to **corrupt or malicious data inputs** This may lead to **- Ethics and Bias** - AI Model drift and performance degradation - Operational disruptions - Compromised threat modeling - myraid of other adverse consequences		- Miss in SLAs or - Attack on Third-party assets - Malicious data inputs to AI/ML models	CISO	4	2	8	Reduce, Share	- ISO/IEC 42001 for AI (since Lemonade is global) OR NIST AI RMF 1.0 - Review SLAs and shared responsibility clauses & use in #3, - AI input validation - validation of third-party AI using - security regressions - functional regressions				
9	DDoS Attack	**Web-interface is attacked by organized botnet** to result in DDoS. This may cause - Service disruption		- Lack of WAF/NGF	CISO	3	2	6	Reduce	- WAF or NG-Firewall				