Cybersecurity Roadmap for Lemonade,Inc.

Saima Ahmed

Current State

Current State:

- Limited In-house IT Security Team (CISO, CIO, 02 Analysts)
- No Formal Cybersecurity Governance
- Cloud Migration Targeting End of 2025
- Global Expansion Plans
- Sensitive Data Handling (Insurance Claims) - Compliance to Regulations (GLBA, GDPR)
- SOC 2 Audit Requirement (2025)

Budget Allocation: 10 Million for 02 years

Industry Benchmarks: For the insurance sector, estimates suggest a range of **6-14%** of IT budget being allocated to security.

Low-End Estimate: 6% of a hypothetical $100 million IT budget to security ~ **$6 million annual.**

High-End Estimate: 14% of a $100 million IT budget, ~ **$14 million annual.**

Risks versus Value Proposition

Top Risks and Threats	Value Proposition
Sensitive Data Leak - The average cost of a data breach in the insurance industry is estimated to be around $7.07 million. **Compromised Credentials** **Lack of Cybersecurity Governance Model** **Non-Compliance -** Non-compliance can result in hefty fines (up to $22 million or 4% of annual global revenue for GDPR) **Cloud Vendor Network Compromise** **AI Model Attacks**	**Enhanced Customer Satisfaction and Trust** **Reduced Risk of Regulatory Fines and Brand Damage** **Reduced Insurance Premiums** **Improved Operational Efficiency** **Strong Security Posture** **Competitive Advantage**

Cost Savings

- Revenue **$ 430 million**- For the Year 2023

- **Conservative Scenario:** Lemonade saves $7.07 million (data breach prevention) + $1 million (avoided fine) = $8.07 million. **This translates to approximately 1.9% of their 2023 revenue**.

- **Optimistic Scenario:** Lemonade saves $9.09 million (data breach prevention) + $1 million (avoided fine) + Revenue retention from 1% reduced churn (difficult to quantify but let's assume it adds another $4.3 million - 1% of their 2023 revenue).
  This translates to a potential revenue increase of 14.3 million or roughly 3.3% of their 2023 revenue.

Business Needs vs. Mitigated Risks/Value to Company

Business Needs

- **Establish Security Governance**
- Improve Security Awareness & Training
- Implement & maintain Access Controls & MFA->**Passwordless Authentication**
- Secure Endpoints, Network, Cloud-> **XDR (Outsourced)**
- Vulnerability Management->**SIEM (Outsourced)->Data Lake**
- Cloud Security Strategy-API
- Third-Party Security Assessments
- **SOC 2 Audit Preparation**
- **AI Security Integration**

Mitigated Risks

- **Lack of Cybersecurity Governance Model**
- **Non-Compliance and Audits**
- **Compromised Credentials**
- **Sensitive Data Leak**
- **Cloud Vendor Network Compromise**
- **AI Model Attacks**

Value to Company

- **Improves compliance posture**
- **Reduces phishing attack success rates**
- **Reduces data breach risk**
- **Improves incident response capabilities**
- **Protects AI models from manipulation and exploitation**

Cybersecurity Program Roadmap (2-Year Phases)

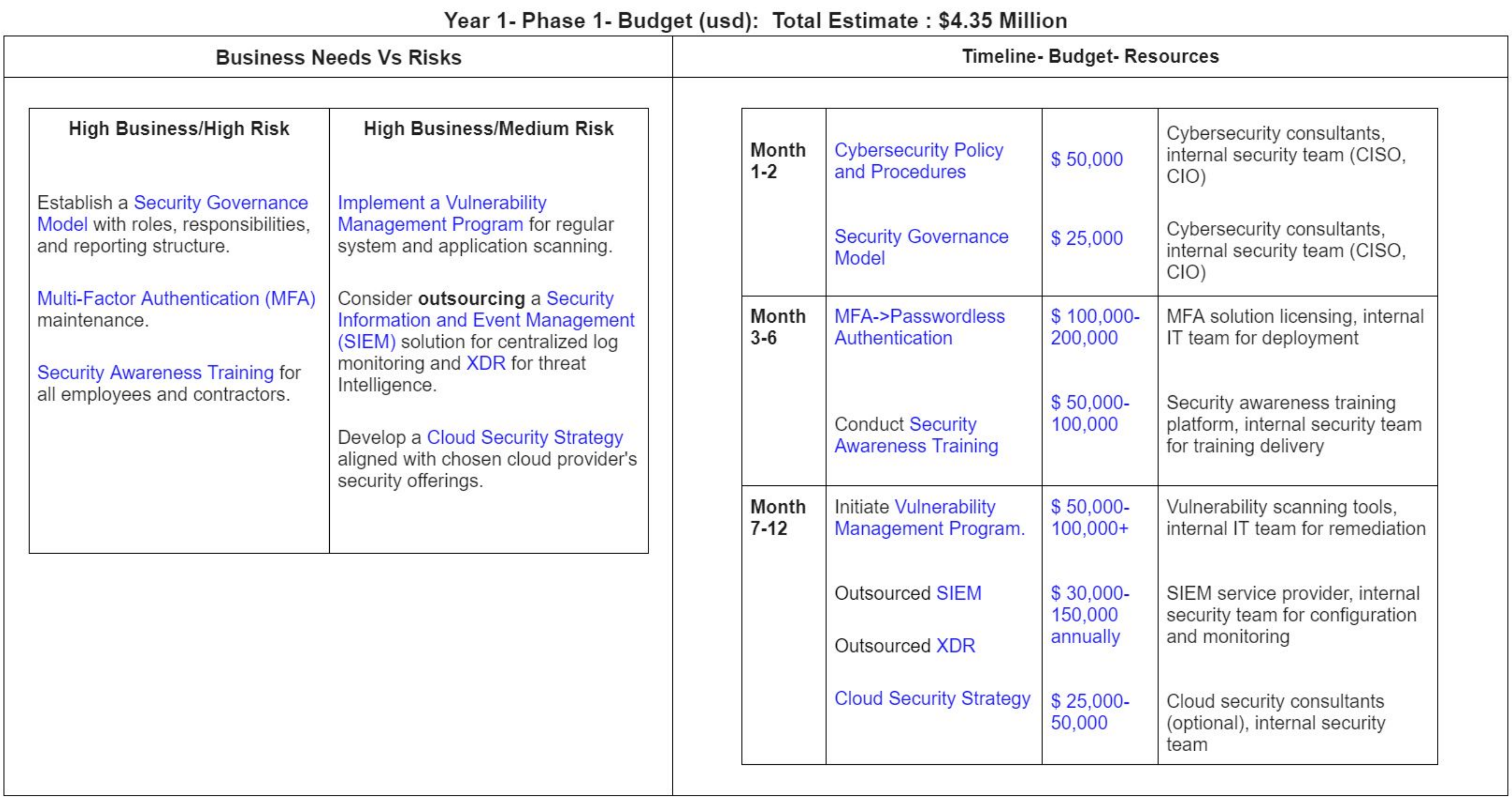
1. Timeline:

- **Year 1 (Phase 1 - Foundation Building):** Focus on establishing core security controls and governance, improve security awareness and prepare for cloud migration.

- **Year 2 (Phase 2 - Advanced Security Measures):** Enhance threat detection and response capabilities, secure cloud environment, and address AI security.

Timeline Overlap:

- **Regular communication with stakeholders,** security awareness training, third-party risk assessments of critical vendors and vulnerability management will be ongoing processes throughout the two years.



Year 1- Phase 1- Budget (usd): Total Estimate : $4.35 Million

Business Needs Vs Risks

High Business/High Risk	High Business/Medium Risk
Establish a Security Governance Model with roles, responsibilities, and reporting structure. Multi-Factor Authentication (MFA) maintenance. Security Awareness Training for all employees and contractors.	Implement a Vulnerability Management Program for regular system and application scanning. Consider **outsourcing** a Security Information and Event Management (SIEM) solution for centralized log monitoring and XDR for threat Intelligence. Develop a Cloud Security Strategy aligned with chosen cloud provider's security offerings.

Timeline- Budget- Resources

Month 1-2	Cybersecurity Policy and Procedures	$ 50,000	Cybersecurity consultants, internal security team (CISO, CIO)
	Security Governance Model	$ 25,000	Cybersecurity consultants, internal security team (CISO, CIO)
Month 3-6	MFA->Passwordless Authentication	$ 100,000-200,000	MFA solution licensing, internal IT team for deployment
	Conduct Security Awareness Training	$ 50,000-100,000	Security awareness training platform, internal security team for training delivery
Month 7-12	Initiate Vulnerability Management Program.	$ 50,000-100,000+	Vulnerability scanning tools, internal IT team for remediation
	Outsourced SIEM Outsourced XDR	$ 30,000-150,000 annually	SIEM service provider, internal security team for configuration and monitoring
	Cloud Security Strategy	$ 25,000-50,000	Cloud security consultants (optional), internal security team

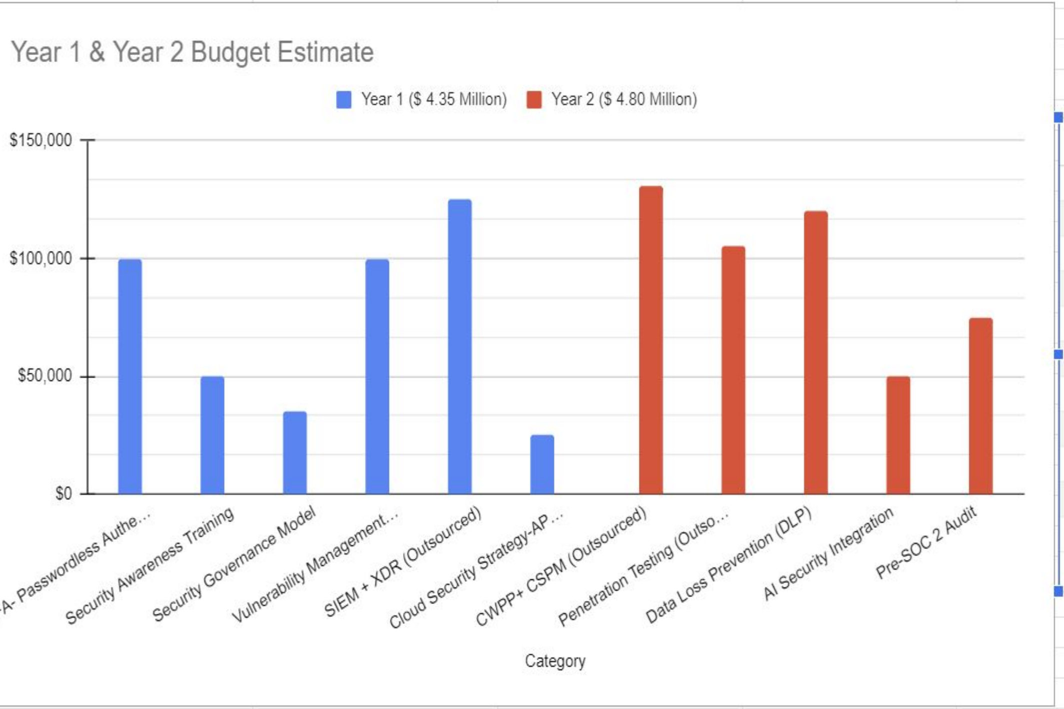
Year 2- Phase 2- Budget (usd): Total : $4.80 Million

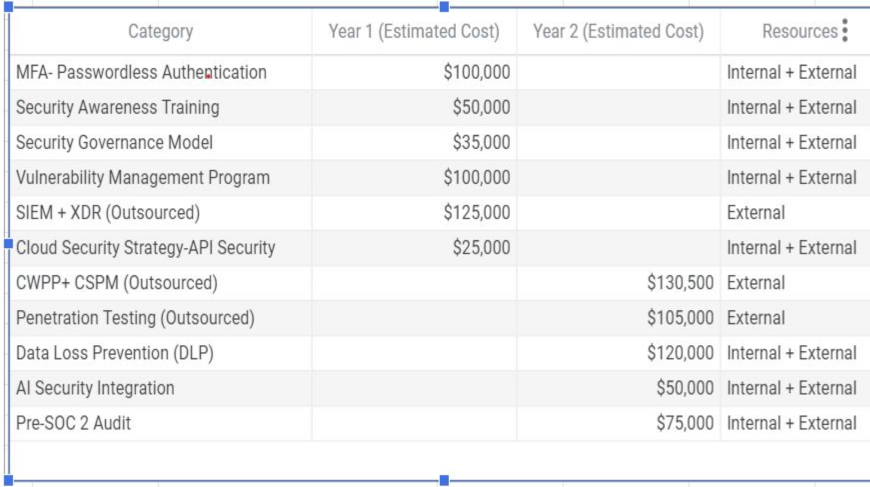
Business Needs Vs Risks

High Business/High Risk	High Business/Medium Risk
Implement Cloud Security Posture Management (CSPM)+ Cloud Workload Protection Platform (CWPP) to monitor and improve cloud environment security Conduct regular Penetration Testing of internal systems and the cloud environment.	Implement Data Loss Prevention (DLP) to prevent sensitive data exfiltration. Integrate AI security best practices. Conduct a pre-SOC 2 audit to identify and address any gaps before the official audit in 2025.

Timeline- Budget- Resources

Month 13-16	Outsourced CWPP+CSPM	$ 75,000 - 100,000 annually)	Cloud security provider, internal security team for configuration and monitoring
	Penetration Testing	$ 50,000 - 100,000 per test	Penetration testing firm, internal security team for remediation
Month 17-20	DLP	$ 100,000 - 200,000+	DLP solution licensing, internal IT team for deployment and policy configuration
	AI security best practices	$ 25,000 - 100,000	AI Security consultants, internal security team
Month 21-24	Conduct a pre-SOC 2 audit.	$ 50,000 - 100,000	Cybersecurity consultants, audit firm, internal security team





Category	Year 1 (Estimated Cost)	Year 2 (Estimated Cost)	Resources
MFA- Passwordless Authentication	$100,000		Internal + External
Security Awareness Training	$50,000		Internal + External
Security Governance Model	$35,000		Internal + External
Vulnerability Management Program	$100,000		Internal + External
SIEM + XDR (Outsourced)	$125,000		External
Cloud Security Strategy-API Security	$25,000		Internal + External
CWPP+ CSPM (Outsourced)		$130,500	External
Penetration Testing (Outsourced)		$105,000	External
Data Loss Prevention (DLP)		$120,000	Internal + External
AI Security Integration		$50,000	Internal + External
Pre-SOC 2 Audit		$75,000	Internal + External

Proactive Security Measures For Future Growth

Lemonade:

- Would continue to **tap third-party security providers for tools** rather than build its own.
- Would continue to improve the proactive end of incident readiness and response- Mitiga, a cloud incident response vendor- not only collects all logs in advance but performs automated, continuous cloud forensics investigations.
- Has moved from **multifactor** to **passwordless authentication**.

Lemonade is now focused:

- On replacing its SIEM with a **Lemonade-developed security data lake**.
- To enhance **API security**.
- Continue to **enhance trust in employees devices**- More can be done.