## Cybersecurity Roadmap with Program Proposal for Lemonade

This roadmap outlines a two-year, phased cybersecurity program for Lemonade, an insurance company undergoing cloud migration and global expansion. Considering the limited in-house security team (CISO, CIO, 2 analysts), the program prioritizes critical controls while leveraging outsourcing for efficiency. It addresses top risks like data leaks, compromised credentials, and cloud security, ensuring compliance and mitigating threats.

**Current State:**

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

| Top Risks and Threats | Value Proposition |
| --- | --- |
| 1. **Sensitive Data Leak:** Potential exposure of customer and financial data.<br>2. **Compromised Credentials:** Phishing attacks, third-party contractor software vulnerabilities.<br>3. **Lack of Cybersecurity Governance Model:** Missing structure for effective security implementation.<br>4. **Cloud Vendor Network Compromise:** Shared responsibility model in cloud requires additional measures.<br>5. **AI Model Attacks:** As AI usage increases, safeguards against manipulation are crucial. | • **Reduced Risk of Data Breaches:** Protects sensitive customer information and financial data-> **Enhanced Customer Satisfaction and Trust**<br>• **Enhanced Regulatory Compliance:** Ensures adherence to data privacy laws and prepares for SOC 2 audit-> **Reduced Risk of Regulatory Fines and Brand Damage**<br>• **Improved Cloud Security:** Mitigates risks associated with cloud migration and global expansion->**Improved Operational Efficiency**<br>• **Stronger Security Governance:** Establishes a framework for effective security implementation-> **Strong Security Posture**<br>• **Cost-Effective Approach:** Leverages outsourcing for efficient program execution->**Competitive Advantage** |

| Business Needs | Mitigated Risks | Value to Company |
|---|---|---|
| **Establish Security Governance** | Lack of Cybersecurity Governance Model & Audits | Ensures clear structure and accountability for security. **Improves compliance posture.** |
| Improve Security Awareness & Training | Compromised Credentials | Empowers employees to identify and avoid security threats. **Reduces phishing attack success rates.** |
| Implement and maintain Access Controls & MFA | Compromised Credentials | Restricts unauthorized access and strengthens login security. **Reduces data breach risk.** |
| Secure Endpoints | Compromised Credentials | Protects devices from **malware** and **data exfiltration**. |
| Vulnerability Management | Sensitive Data Leak,<br>Cloud Vendor Network Compromise | Identifies and patches vulnerabilities in systems and applications to **prevent exploitation.** |
| Cloud Security Strategy | Cloud Vendor Network Compromise | Proactive measures to secure data and applications within the cloud environment. **Aligns with cloud provider's security offerings**. |
| Third-Party Security Assessments | Compromised Credentials | Evaluates security posture of vendors and **mitigates potential risks associated with third-party access.** |
| **SIEM (Outsourced), XDR(Outsourced)** | Sensitive Data Leak, Compromised Credentials | Centralizes logs for real-time monitoring and threat detection. **Improves incident response capabilities**. |
| **SOC 2 Audit Preparation** | Lack of Cybersecurity Governance Model & Audits | **Ensures compliance** with relevant standards **and prepares for successful audit in 2025.** |
| **AI Security Integration** | AI Model Attacks | **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 and vulnerability management will be ongoing processes throughout the two years.
- Third-party security risk assessments of critical vendors can be conducted throughout the program.

## 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.<br><br>Multi-Factor Authentication (MFA) maintenance.<br><br>Security Awareness Training for all employees and contractors. | Implement a Vulnerability Management Program for regular system and application scanning.<br><br>Consider **outsourcing** a Security Information and Event Management (SIEM) solution for centralized log monitoring and XDR for threat Intelligence.<br><br>Develop a Cloud Security Strategy aligned with chosen cloud provider's security offerings. |

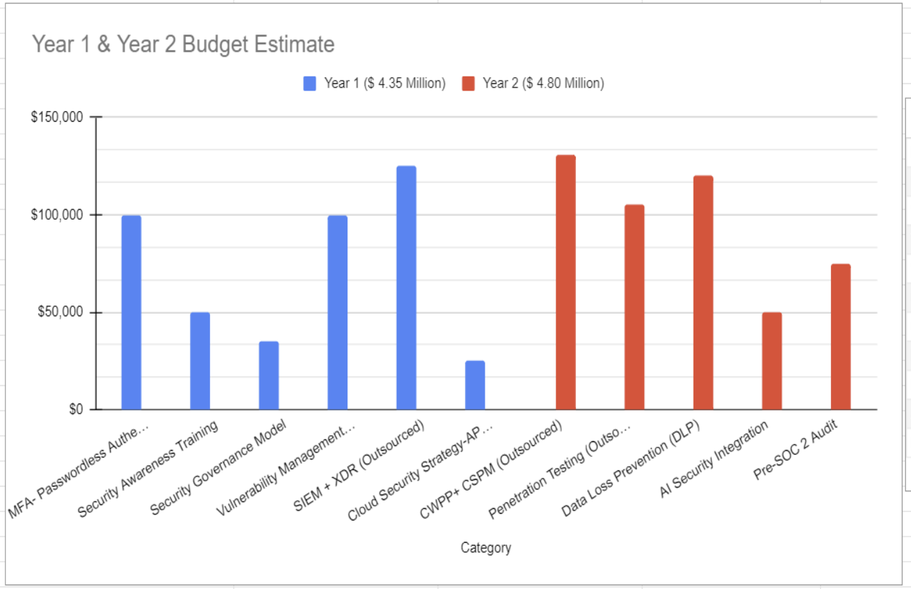
### Timeline- Budget- Resources

| | | | |
|---|---|---|---|
| **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<br>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<br><br>Conduct regular Penetration Testing of internal systems and the cloud environment. | Implement Data Loss Prevention (DLP) to prevent sensitive data exfiltration.<br><br>Integrate AI security best practices.<br><br>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<br><br>Penetration Testing | $ 75,000 - 100,000 annually)<br><br>$ 50,000 - 100,000 per test | Cloud security provider, internal security team for configuration and monitoring<br><br>Penetration testing firm, internal security team for remediation |
| **Month 17-20** | DLP<br><br>AI security best practices | $ 100,000 - 200,000+<br><br>$ 25,000 - 100,000 | DLP solution licensing, internal IT team for deployment and policy configuration<br><br>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 |

**Stakeholder Alignment and Feedback Loop :**

- **Stakeholder Engagement:** Work closely with executives, IT leaders, legal teams, and employees to align security with business goals.
- **Regular Reviews:** Conduct periodic check-ins to assess progress, gather feedback, and adapt the plan as needed.
- **Continuous Improvement:** Seek input from employees and external experts to ensure the program remains effective against evolving threats.
- **Flexibility:** Maintain a flexible approach to address changing security landscapes and business needs.

**Backup Strategies:**

- **Phased Implementation:** Prioritize controls based on risk and implement them in phases to minimize disruption and allow for adjustments as needed.
- **Open-Source Alternatives:** Consider open-source security tools where commercially viable options exceed the budget.
- **Internal Resource Training:** Train internal IT personnel on security best practices to build internal expertise and reduce reliance on external resources.
- **Regular Communication and Risk Assessments:** Maintain open communication with stakeholders and conduct ongoing risk assessments to identify and address emerging threats throughout the program's lifecycle.

**References:**

https://en.wikipedia.org/wiki/Lemonade,_Inc

https://www.itprotoday.com/compliance-and-risk-management/developing-proactive-security-measures-lessons-lemonade

https://orca.security/resources/case-studies/insurance-innovator-lemonade-goes-from-0-to-100-cloud-visibility-with-orca-security/

https://businessmodelanalyst.com/lemonade-business-model/